TIETOTURVAN AUDITOINTIMAHDOLLISUUDET IOT-ALUSTOISSA

ISO 27001- standardi

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ylemmän ammattikorkeakoulututkinnon opinnäytetyö

Älykkäät palvelut digitaalisessa toimintaympäristössä, Visamäki

kevätlukukausi 2021

Harri Hamberg

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Älykkäät palvelut digitaalisessa toimintaympäristössä Tiivistelmä

Hämeenlinnan korkeakoulukeskus

Tekijä	Harri Hamberg	Vuosi 2021
Työn nimi	Tietoturvan auditointimahdollisuudet IoT-alustoissa - ISO 27001-standardi	
Ohjaajat	Jari Jussila	

TIIVISTELMÄ

Tässä tutkimuksessa selvitettiin, miten hyvin ISO 27001-standardi informaatio turvallisuuden hallintajärjestelmä (Information Security Management System, ISMS) ottaa huomioon auditoinneissa IoT-järjestelmät ja näihin kohdistuvan riskienhallinnan. Tutkimus toteutettiin kvalitatiivisena tapaustutkimuksena. Haastattelut kohdistettiin kuuteen haastateltavaan, joista neljä edusti akkrekoituja auditoijia ja kaksi yritysedustajia.

Tutkimus osoitti, että IoT-laitteiden heterogeenisyys aiheuttaa riskien hallintaongelmia auditoinnin kohteena olevalle organisaatiolle. Heterogeenisyys vaikeuttaa auditoinnin päämäärän toteutumista, koska haavoittuvuuksien ja riskitekijöiden löytäminen vaikeutuu. IoT-alusta voi koostua hyvin erilaisista laitteista, joiden tarkkaa toimintaa, ominaisuuksia ja liitettävyyttä ei järjestelmää käyttävä organisaatio välttämättä tunne tai tunnista. Nämä seikat eivät tule järjestelmällisesti esiin auditoinneissa, koska hallintajärjestelmien rajaus aiheuttaa turvallisuuspuutteita. IoT-alustojen riskienhallintaan voidaan vaikuttaa tehokkaalla muutoksenhallinnalla ja havainnointikyvyllä. Proaktiivisessa ajattelutavassa pienimmätkin muutokset yrityksen toiminnassa tai toimintatavassa tulee analysoida riskipohjaisesti ja ennakkoluulottomasti. ISO 27001-standardin kansainvälinen uudistamisprosessi on liian hidas, verrattaessa IoT-ekosysteemin nopeasykliseen kehittymiseen. Myös ISO 27001-standardin liitettä A pidetään yleisesti riittämättömänä IoT-ekosysteemien riskien tarkasteluun ja lisästandardin tarve on ilmeinen.

Avainsanat	ISO 27001-standardi, IoT, Riskienhallinta, Tietoturva, Auditointi
Sivut	70 sivua ja liitteitä 2 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Smart Services in Digital Environment **Abstract**

Hämeenlinna University Centre

Author	Harri Hamberg	Year 2021
Subject	Security auditing capabilities on IoT platforms-ISO 27001 Standard	
Supervisors	Jari Jussila	

ABSTRACT

This study examined how well the ISO 27001 standard (Information Security Management System, ISMS) takes into account IoT systems and their risk management during auditing. It was conducted as a qualitative case study. The interviews focused on six interviewees, four of whom represented accredited auditors and two company representatives.

The study showed that heterogeneity of IoT-devices causes risk management problems for the organization under audit. Heterogeneity makes achieving the objective of auditing difficult, as it complicates finding vulnerabilities and risk factors. An IoT platform can consist of very different devices, the exact functioning, features and connectivity of which the organization using the system may not know or recognize. These issues do not systematically arise during auditing, because the demarcation of management systems causes security deficiencies. The risk management of IoT platforms can be improved by effective change management and perception. A proactive mindset analyses even the smallest changes in the company's operations or procedures in a risk-based and unbiased way. The international renewal process of the ISO 27001 standard is too slow in comparison to the rapid cyclical development of the IoT ecosystem. Appendix A to the ISO 27001 standard is also generally considered insufficient for examining the risks of IoT ecosystems, and the need for an additional standard is clear.

Keywords	ISO 27002-standard, IoT, Risk Management, Information Security, Audit
Pages	70 pages and appendices 2 pages

Sisällys

1 Johdanto ... 1
1.1 Tausta ja motivaatio ... 2
1.2 Tutkimuksen tavoite ja tutkimuskysymykset ... 3
1.3 Aihepiirin rajaukset ja aiemmat tutkimukset ... 6
1.4 Keskeisten käsitteiden määrittely ... 7
2 IoT-ekosysteemi ... 8
2.1 Lainsäädäntö ja ohjeistus ... 9
2.1.1 Riskienhallinnan standardit ja ohjeistus ... 10
2.1.2 ISO 27001 -standardi ... 10
2.2 IoT-alustat ... 12
2.2.1 IoT-alustojen haasteet ... 12
2.2.2 IoT-alustojen mahdollisuudet ... 13
2.3 Tietoturva ... 14
2.3.1 Tietoturvan uhkat ... 15
2.3.2 Tietoturvan haasteet ... 16
2.3.3 Tietoturvan tavoitteet ... 17
2.4 Riskienhallinta ... 17
2.4.1 Riskienhallinnan haasteet ... 18
2.4.2 Riskienhallinnan hyödyt ... 19
2.5 Auditointi ... 20
2.5.1 Auditoinnissa havaitut haasteet ... 21
2.5.2 Tietoturva-auditoinnin hyödyt ... 22
3 Tutkimuksen kuvaukset ja menetelmät ... 23
3.1 Tutkimusstrategia ... 23
3.2 Tiedonhankinnan strategia ... 24
3.3 Aineiston kerääminen ... 25
3.4 Tutkimuksen luotettavuuden arviointi ... 29
3.5 Aineiston analysointi ... 31
4 Tutkimustulokset ... 32
4.1 Lainsäädäntötarpeet ... 33
4.2 IoT-alustojen turvallisuusnäkökohtien ajantasaisuus ... 36
4.3 Riskienhallinnan ja tietoturvan huomioiminen ... 41
4.4 Auditointikäytännöt ... 47

5 Tulosten tarkastelu, pohdinta ja johtopäätökset 53
5.1 Lainsäädännön ja ohjeistuksen näkökulma 53
5.2 Tietoturvan ja riskienhallinnan moninaisuus 55
5.3 Auditoinnin vaikutus hallintajärjestelmään 56
5.4 Johtopäätökset 58
5.5 Tulosten yleistettävyys ja käytännön suositukset 63
LÄHTEET 65

Liitteet

Liite 1 Gioia-metodi
Liite 2 Haastattelukysymykset

1 Johdanto

Esineiden internet (myöhemmin IoT) tulee muuttamaan yhteiskuntaa yhtä voimakkaasti kuin internet aikoinaan. IoT:n läpilyövä luonne luo yhteiskunnalle monia etuja, mutta myös haasteita. (Nurse ym., 2018, s. 1) Terminä ”Internet of Things” on laaja ja sen nähdään kattavan suuren määrän monenlaisia älykkäitä sovelluksia, esimerkiksi erilaiset järjestelmien rajapinnat (Singh ym., 2016, s. 3).

IoT edustaa verkottuneiden objektien kommunikointia datan avulla, joita on mahdollista hallita muilla laitteilla, järjestelmillä ja palvelimilla. Esineiden, ihmisten ja verkkojen väliseen viestintään liittyy tietoisia ja tiedottamattomia toimia yhdestä IoT-laitteesta toiseen IoT-laitteeseen tai niin sanottuun agenttiin. Tämä erottaa internetin toiminnan asioiden internetistä. IoT:ssä ihmisen ja automaation vaikutus vähenee, joka on taas internetissä toiminnan edellytys. (Hejazi ym., 2019, s. 1)

IoT tunnetaan digitaalitalouden nimellä neljäs teollinen vallankumous. Se tuo uusia toimintariskejä yhdistetyille digitaalisille kyberverkoille ja lisäävät usein vakavasti turvallisuusriskiä sekä nostavat tärkeitä eettisiä huolia. (Radanliev ym., 2019b, s. 1) Jatkuva teknologian sekä automaation yleistyminen monimutkistavat IoT:n toimintaympäristöä. Riskienarvioinnin arvioinneille ja luottamuksen rakentamiselle tarvitaan uusia lähestymistapoja. (Nurse ym., 2017, s. 1)

Tietoturvan hallintajärjestelmästandardi ISO/IEC 27001 on tietoturvallisuuteen liittyvä virallinen vaatimusstandardi. ISO 27001-standardi on kansainvälisesti yksi tunnetuimmista ja käytetyimmistä organisaation tietoturvallisuuden hallinnan standardeista. Standardi rakentuu perusosasta sekä liitteestä A, joka pitää sisällään esimerkkikontrollit. (Traficom, 2019, 8) Auditointiprosessit, päätehtävänä on suunnitella, kehittää ja ottaa käyttöön järjestelmä, jolla pystytään keräämään- ja havainnoimaan erilaisia suojaustason vaihteluita sekä tapahtumia laitteista ja järjestelmistä (Matheu-Garcia ym., 2018, s. 16).

1.1 Tausta ja motivaatio

Palvelualustojen ympäristössä on havaittavissa kohdentamattomia tietoturvahaasteita. IoT-laitteet lisääntyvät huimaa vauhtia erilaisilla palvelualustoilla, jolloin myös laitteiden tietoturvaan ja auditointiin tulee kiinnittää erityistä huomiota. Tämän tutkimuksen tekijä on havainnoinut tilanteita, joissa erilaisia tietoturvaa huonosti huomioonottavia laitteita pyritään liittämään IoT-alustaan. Näiden laitteiden tietoturvasta ei tämän tutkimuksen tekijän näkemyksen mukaan ole takeita. Tutkija näkeekin, että laitteiden ominaisuuksien tutkiminen on erittäin haastavaa nykyisillä tietoturva- ja riskienhallintatyökaluilla. Vakavat tietoturvariskit voivat jäädä tunnistamatta joissain tapauksissa.

Palvelutarjoajien yleistyvänä käytäntönä on, että yritykset ottavat käyttöön hybridi-palvelualustan, jossa osa datasta siirretään kansainvälisen toimijan kaupalliseen pilvipalveluun. Tämä tuo tutkimuksen tekijän mukaan aivan uudenlaisen tietoturvan riskienhallinnan haasteen organisaatiolle, vaikka käytetty palvelu olisikin ISO 27001-standardin mukaisesti auditoitu ja sertifioitu ulkoisen akkretoidun auditoijan toimesta. Duncan ja Whittington (2016, s. 125) toteavat, että turvallisuus saavutetaan yleensä noudattamalla standandeja, lisäämällä toimintavarmuutta sekä turvallisuutta auditoinneilla. Turvallisuusnäkökohdat ovat selkeitä perustilanteessa, jossa ei toimita IoT-pilvessä. Siirryttäessä IoT-pilvipalveluihin, turvallisuusnäkökohdat muuttuvat täysin. (Duncan & Whittington, 2016, s. 125)

Kun tarkastellaan ISO 27001- standardin ajantasaisuutta IoT-pilvipalvelualustojen auditoinnissa, tutkimuksen tekijä nostaa esiin kysymyksen standardin vaatimusten ajantasaisuudesta erilaisista tietoturvanäkökulmista, joita IoT-alusta aiheuttaa toiminnassa. Vanhojen menetelmien soveltaminen uudenlaisiin uhkiin voi vaikuttaa negatiivisesti riskeihin, jotka nousevat uusista ekosysteemeistä (Nurse ym., 2017, s. 1). IoT:n haaste turvallisuus- ja luottamuksenhallinnan näkökulmasta on kuitenkin se, että olemassa olevat riskinarviointimenetelmät rakennettiin ennen IoT-alustojen kehittymistä, joten ne eivät välttämättä vastaa näiden automatisoitujen järjestelmien monimutkaisuutta (Nurse ym., 2017, s. 1).

ISO 27001- auditointeja ja seuranta-auditointeja tehdään organisaatioissa suunnitelluin väliajoin tai merkittävien muutoksien tapahtuessa (SFS-EN ISO/IEC 27001/2017, s. 27). Tämän tutkimuksen tekijä nostaa esiin aikaperiodikysymyksen uusien tietoturvalaitteiden auditoinnissa. Myös kysymys ISO 27001-standardin riittävän monipuolisesta käytettävyydestä pilvipalvelualustojen auditoinneissa on herättänyt keskustelua, kuten myös tarpeeksi kattavan uudenlaisten tietoturvariskien huomioiminen toiminnassa, joita heterogeeninen järjestelmäympäristö aiheuttaa.

Aiemmin tuntemattomien IoT-järjestelmien liittäminen osaksi organisaation nykyistä ympäristöä muodostaa riskin, joka vaatii tämän tutkimuksen tekijän mukaan tehokasta muutoksenhallintaa. Tässä oleelliseksi asiaksi tutkimuksen tekijän mukaan nousee muutoksenhallinnan juurisyiden havainnointi vaadittujen standardien mukaisesti. Nurse ym., (2017, s. 5) korostavat riskinarvioinnin ennustettavuutta ja harkintaa järjestelmien osalta, jotka saattavat ilmetä ennen seuraavaa määräaikaisarviointia. Nurse ym. (2017, s. 5) jatkavat ja toteaa, että riskiarvioinnit ovat epäpäteviä niiden jaksottaisen arvioinnin vuoksi ja toteavat tämän olevan huomattava heikkous arvioitaessa IoT-riskejä. Myös Duncan ja Whittington (2016, s. 125) ovat havainneet johdonmukaisten pilvistandardien puuttumisen korostavan pilvipalvelun tarkastuksen tehokkuutta ja prosessin perustavanlaatuista heikkoutta.

1.2 Tutkimuksen tavoite ja tutkimuskysymykset

Tämän opinnäytetyön tavoitteena on selvittää, miten hyvin ISO 27001-standardi (Informaatio turvallisuuden hallintajärjestelmä, ISMS) ottaa huomioon IoT-järjestelmät ja näihin kohdistuvan riskienhallinnan. Suomen johtavien auditointiyritysten virallisten akkrekoitujen auditoijien avulla selvitettiin mahdollisia tunnistettuja heikkouksia IoT-laitteita sisältävien hallintajärjestelmien ISO 27001-standardin auditoinneissa. Tutkimukseen osallistui myös yksityisten yritysten IoT-asiantuntijoita, joiden roolina tässä tutkimuksessa oli arvioida ISO 27001- standardin ominaisuuksien soveltuvuutta yritysten näkökulmasta IoT-alustoja sisältäviin hallintajärjestelmiin.

ISO 27001-standardin heikkoutena pidetään A-liitettä sekä sovelluslausuntojen merkityksiä, jotka eivät ole selkeitä, vaatimukset ovat ympäripyöreitä ja hankalasti tulkittavia (Traficom,

2019). Lisäksi tässä opinnäytetyössä tutkitaan ISO 27001-standardin hallinnollisten vaatimusten soveltuvuutta IoT-alustojen tietoturvaominaisuuksien havainnoinnissa sekä selvitetään erilaisia muutoksenhallinnan havainnointimenetelmiä IoT-alustoissa.

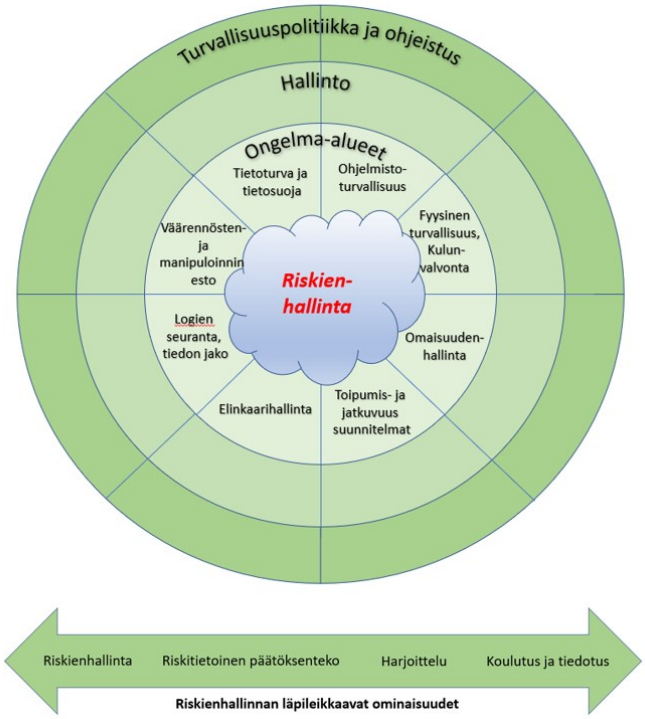
Vaikka ISO 27001-standardi ei ole varsinainen tietoturvastandardi vaan hallinnan ja johtamisen standardi, se antaa viitekehyksen sekä riskiperustaisen näkymän siihen, miten organisaatiossa hallitaan tietoturvallisuuteen sisältyviä ja liittyviä asioita. ISO 27001-standardi on oikeastaan ainoa ja yksi tunnetuimmista sekä käytetyimmistä organisaation tietoturvallisuuden hallinnan standardeista. (Traficom, 2019) Huomioitavaa on, että ISO 27001-standardi koostuu joukosta erilaisia vaatimuksia, jotka ovat niin yleisiä, että ne sopivat lähes jokaiselle organisaatiolle toimialasta tai koosta riippumatta. Edellä mainitun takia standardista on muodostunut erittäin suosittu ja kansainväliset asiakkaat vaativat usein tämän standardin noudattamista. (Traficom, 2019)

Oracevic ym. (2017) viittaavat tutkimuksessaan haasteisiin, jotka johtuvat IoT-järjestelmien puutteista tietoturvasuojauksessa; miten organisaatioissa huomioidaan heterogeenisten laitteiden standardointi, laaja käyttöönotto ja skaalautuvuus, luottamuksellisuus, laitteistohaavoittuvuudet, fyysinen turvallisuus sekä energiankulutus ja tehokkuus. Myös Nurse ym. (2017, s. 1) toteavat, että uusien järjestelmien ekosysteemien käyttöönottovaiheessa voidaan olla sokeita uusille riskeille, jotka muodostuvat erilaisten järjestelmien korkeasta yhteysasteesta, erilaisista tietoverkoista, fyysisten ja sosiaalisten järjestelmien kytkeytyessä toisiinsa.

Tietoturvallisuuden riskienhallintaan liittyvät keskeiset kokonaisuudet; eheys, käytettävyys ja saatavuus tulee huomioida järjestelmien turvallisuudessa. Myös turvallisuuspolitiikka ja ohjeistus antavat viitekehyksen yrityksen tietoturvatoiminnoille. (DiMase ym., 2015, s. 291) DiMasen ym. (2015, s. 293) mukaan riskien ymmärtäminen ja arvioiminen omassa organisaatiossa onnistuneesti, vaatii verkkoympäristön täydellistä ymmärtämistä. Yrityksen hallinnossa ohjeistusta kehitetään riskienhallinnasta saatujen havaintojen perusteella. Hallinnon toiminta-alueelle kuuluu myös tietoturvaohjeistuksen jalkauttaminen yrityksen henkilökunnalle. (DiMase ym., 2015, s. 292–293).

DiMasen ym. (2015, s. 294) mukaan järjestelmän turvallisuus koostuu useasta erilaisesta ongelma-alueesta, jotka on huomioitava järjestelmien riskienhallinnassa ja suunnittelussa. Näitä osa-alueita ovat ohjelmistoturvallisuus, fyysinen turvallisuus ja kulunvalvonta, omaisuudenhallinta, toipumis- ja jatkuvuussuunnitelmat, elinkaarihallinta, logien seuranta ja tiedonjako, väärennösten ja manipuloinnin esto ja viimeisenä tietoturva ja tietosuoja. Nämä osa-alueet on kuvattu soveltaen kuvassa 1.

Kuva 1. Riskienhallinnan keskeiset vaatimukset, soveltaen. (DiMase ym., 2015, s. 294)



Tämän tutkimuksen päätutkimuskysymys on seuraava:

1. Miten ISO 27001-standardin vaatimukset vastaavat IoT-alustojen riskeihin?

Alatutkimuskysymykset:

2. Miten IoT-alustojen heterogeenisyys otetaan huomioon auditoinneissa?
3. Minkälaisia riskien havainnointimenetelmiä IoT-pilvipalveluissa on mahdollista käyttää?

Kun tarkastelemme innovatiivisuuden näkökulmasta aihevalintaa, tutkimuksen tekijä kokee tutkimuksen tuovan uusia mahdollisuuksia niin palveluliiketoiminnalle kuin IoT-tietoturvan huomioimiseen erilaisissa digitaalisissa palveluissa. Tutkimus antaa näkökulmaa palvelujen käyttäjien ja tuottajien entistä paremman tietoturvatason huomioimiseen IoT-alustoissa. Tämän tutkimuksen tekijä toteaa turvallisen palveluympäristön mahdollistavan lisää toimeksiantoja asiakkailta. Pidemmällä aikajaksolla turvallinen toimintaympäristö on tuottavampi, kuin heikoilla turvallisuusominaisuuksilla varustettu ympäristö. Kustannukset aiheutuvat monesti tietomurtojen tai laitteiden asetusten tahattomien muutosten korjaustarpeista.

1.3 Aihepiirin rajaukset ja aiemmat tutkimukset

Teoreettinen viitekehys muodostuu tietoturvan ja riskienhallinnan aiempien tutkimusten perusteella. Tutkimuksessa on oleellista ymmärtää, mitkä tekijät toimintaympäristössä vaikuttavat erityisesti uusien, ennalta tuntemattomien, äkillisten riskien muodostumiseen ja miten niitä voidaan hallita.

IoT- järjestelmiin kohdistuvia riskejä on kansainvälisesti tutkittu usean eri tutkijan ja tutkijaryhmien toimesta viime vuosien aikana. Tässä tutkimuksessa on käytetty uusimpia tieteellisiä julkaisuja tietoturvaan ja riskienhallintaan liittyvistä aihepiireistä. Tutkijat ovat havainneet useissa tutkimuksissa, että monimutkaisissa IoT-laitteita sisältävissä järjestelmissä hyvä tietoturva ja riskienhallinta toteutuvat heikosti. Keskeisiä artikkeleita IoT-riskienhallinnan osalta, ovat kirjoittaneet muun muassa:

Radanliev, Nurse ja De Roure yhdessä tutkimusryhmiensä kanssa. Esimerkkinä tieteelliset artikkelit: If you can´t understand it, you can´t properly assess it! (Nurse, Radanliev, Creese, De Roure, 2018) sekä Cyber risk in IoT systems (Radanliev, De Roure, Maple, Nurse, Nicolescu, Ani, 2019).

IoT:n tietoturvaa on tutkinut muun muassa Atlam ja Wills artikkelissaan: IoT security, Privacy, Safety and Ethics, 2019. Myös Radanliev tutkimusryhmänsä kanssa on tutkinut IoT-laitteiden tietoturvaa useassa eri tutkimuksessa, kuten esimerkiksi; Cyber Security

Framework for the internet-of-things in Intrustry 4.0 (Radanliev, De Roure, Nurse, Nicolescu, Huth, Cannady, Mantilla Montalvo, 2019).

Auditoinnin näkökulmaa IoT-laitteita sisältäviin järjestelmiin on tutkinut muun muassa Saleem tutkimusryhmänsä kanssa, tästä esimerkkinä IoT Standardisation – Challenges, Perspectives and Solution (Saleem, Hammoudeh, Raza, Abebisi ja Ruth, 2018). Lisäksi IoT-alustoja ovat käsitelleet tutkimuksissaan muun muassa Nicolescu, Huth, Radanliev ja De Roure; julkaisussaan Mapping the values of IoT, 2018.

Tässä opinnäytetyössä ei tutkita IoT:n hallinnointi- ja johtamismahdollisuuksia, eikä IoT-alustojen ominaisuuksia. Myös koti-IoT-järjestelmät rajataan tämän tutkimuksen ulkopuolelle.

1.4 Keskeisten käsitteiden määrittely

Seuraavaksi tuodaan esille tutkimuksen keskeiset käsitteet.

Auditointi	Auditoinnilla tarkoitetaan myös sertifiointia, jossa riippumaton akkretoitu taho arvioi virallisesti palvelua, tuotteita ja prosesseja määritettyjä kriteerejä ja standardeja vasten. Auditoinnin tuloksena loppukäyttäjät voivat vakuuttua tieto- ja viestintätekniikan tuotteiden ja palveluiden turvallisuusominaisuuksista. (Kyberturvallisuusasetus, 2017, s. 10)
IoT	IoT- koostuu erilaisista heterogeenisista pilvitekniikoista, jotka ovat elinkaaren erilaisissa vaiheissa olevia IoT-laitteita (Radanliev ym., 2020). IoT kattaa hyvin laajan sovellusvalikoiman, jolloin filosofiana on kaiken tekniikan laaja integrointi (Singh ym., 2016, s. 1).
ISO 27001-standardi	SFS-EN ISO/IEC 27001:2017 on kansainvälinen tietoturvallisuuden hallintajärjestelmän standardi. (SFS-EN ISO/IEC 27001/2017, s. 4) ISO ja IEC muodostavat maailmanlaajuisen standardointiin erikoistuneen järjestelmän, joiden kansalliset jäsenjärjestöt eri

maissa osallistuvat kansainvälisten standardien laadintaan näiden teknisissä komiteoissa, joissa käsitellään tekniikan eri osa-alueita. (SFS-EN ISO/IEC 27001/2017, s. 4)

Lainsäädäntö	Lainsäädännöllä tarkoitetaan kansallisia tai EU tason asetuksia, jotka asettavat tietoturva vaatimuksia erilaisille tietoteknisille järjestelmille. Tällainen on muun muassa kesäkuussa 2019 voimaan astunut EU:n kyberturvallisuusasetus (Traficom, 2019). Toinen EU tasoinen asetus on EU:n tietosuoja-asetus (GDPR), joka kohdistuu tietosuojakäytäntöihin ja joka velvoittaa jokaista EU-alueella toimivaa yritystä tai yhteisöä (Saleem ym., 2018).
Riskienhallinta	Riskienhallinnassa tehdään erilaisten riskien arviointia, kuten tunnistamista ja priorisointia, joilla tunnistetaan organisaatioon tai toimintaan vaikuttavat kaikki tekijät, kuten uhat, erilaiset haavoittuvuudet ja niiden vaikutukset. (Nurse ym., 2018, s. 2; Nurse ym., 2017, s. 2)
Tietoturva	Tietoturvan peruskäsitteinä pidetään luottamuksellisuutta, eheyttä, ja saatavuutta (Duncan ym., 2016, s. 125). Luottamuksellisuus tarkoittaa erilaisten viestien vaihtoa lähettäjän ja vastaanottajan välillä, jotka on suojattava vahingollisilta ja todentamattomilta käyttäjiltä. Eheydellä taataan lähettäjän ja vastaanottajan välisten viestien sisältö, joka on suojattu tunkeilijan mahdolliselta manipuloinnilta. Saatavuutta käytetään takaamaan pahantahtoisen käyttäjän häirintä tai vahingoittaminen, joka liittyy lähettäjän ja vastaanottajan viesteihin tai palvelun laatuun. (Atlam & Wills, 2019, s. 129)

2 IoT-ekosysteemi

IoT mahdollistaa nykyisen ympäristön kehittämisen uusilla toiminnoilla, kuten mahdollistamalla älykkäitä kaupunkeja, verkkoja ja erilaisia automaattisia ympäristöjä sekä

niiden analysoinnin. IoT ei tunne maantieteellisiä, poliittisia tai taloudellisia rajoitteita. (Minerauda ym., 2016, s. 1; Nicolescu ym., 2018, s. 346) IoT-alustat tarjoavat myös monipuolisia ominaisuuksia teollisuuden käyttöön, mahdollistamalla esimerkiksi joustavuutta suunnittelijoiden ja toteuttajien päätöksentekoon (Hejazi ym., 2018).

IoT-laitteita sisältävien järjestelmien riskienhallinnassa ilmenee erilaisia haasteita sekä aikaisemmin tunnistamattomia riskejä. Kohdeorganisaatiolle on tärkeää ymmärtää riskienhallinnan kehittämisen hyödyt. (Hejazi ym., 2018) IoT:n yksi suurimmista haasteista tietoturvassa on resilienssi, joka tarkoittaa järjestelmien kykyä vastata IoT-järjestelmään kohdistuvista, ennakoimattomista hyökkäyksistä tai tilanteista joustavasti ja toipua niistä (Atlam & Wills, 2019, s. 137).

Riippumattomilla akkretoidulla sertifioinneilla (auditointi) arvioidaan tuotteet, palvelut ja prosessit määritettyjen kriteereitä ja standardeja vasten, joista annetaan sertifikaatti vaatimuksen mukaisuudesta. Tällä on tärkeä merkitys tuotteiden ja palveluiden turvallisuuden sekä luotettavuuden lisäämisessä. (Kyberturvallisuusasetus, 2017, s. 10)

2.1 Lainsäädäntö ja ohjeistus

IoT-tietoturvaan ei ole olemassa tällä hetkellä erityisiä säännöksiä, jolloin IoT:n käyttöön saattaa liittyä monia oikeudellisia kysymyksiä. EU:n yleinen tietosuoja-asetus (GDPR) asettaa tiukat vaatimukset henkilötietojen keräämiselle ja käsittelylle. (Nurse ym., 2018, s. 7) Yritysten onkin tiedettävä hyvin tarkkaan mitä dataa käyttöön otettu IoT-järjestelmä kerää ja miten riskienarvioinnit soveltuvat niihin (Nurse ym., 2018, s. 7).

Tärkeimpiä IoT:n kasvua sekä käyttöönottoa rajoittavia tekijöitä ovat standardoitujen työkalujen puuttuminen järjestelmäalustoissa ja rajapinnoissa. Työkalut mahdollistavat erilaisten ratkaisujen tarjoamisen laitteisto- ja ohjelmatoimittajien välillä. (Sicari ym., 2016, s. 44) Velvoitteita jonkin tietyn turvallisuustekniikan käyttöön ei Pasquierin ym., (2017, s. 336) mukaan IoT-järjestelmissä tällä hetkellä ole, he näkevät, että auditoinnilla voidaan osoittaa tarvittavien turvallisuustoimenpiteiden toteutus asianmukaisesti.

2.1.1 Riskienhallinnan standardit ja ohjeistus

Erilaisilla verkko-, tietojärjestelmillä ja televiestiverkoilla sekä palveluilla on yhteiskunnassa elintärkeä rooli, joka myös mahdollistaa talouskasvua (Kyberturvallisuusasetus, 2017, 24). Erilaiset tieto- ja viestitekniikat mahdollistavat pohjan monimutkaisille järjestelmille, jotka tukevat yhteiskunnan erilaisia toimintoja, mahdollistavat talouden toimivuuden ja tukevat sisämarkkinoiden toimintaa (Kyberturvallisuusasetus, 2017, s. 24).

Erilaisten verkko- ja tietojärjestelmien käyttö on levinnyt laajalle Euroopan unionissa, jolloin erilaiset digitaalisuus ja verkkoyhteydet ovat keskeisiä ominaisuuksia tuotteissa ja palveluissa (Kyberturvallisuusasetus, 2017, s. 24). On ennakoitu, että IoT- laitteita liitetään internettiin EU:n alueella miljoonia tai jopa miljardeja seuraavan kymmenen vuoden aikana. Järjestelmien ja laitteiden turvallisuuteen ja resilienssiin pitää kiinnittää erityistä huomiota, jotta vältytään kyberturvallisuuteen liittyvien puutteiden ongelmista. (Kyberturvallisuusasetus, 2017, s. 24) Sertifioinnin vähäinen käyttö johtaa siihen, että erilaiset organisaatiot ja käyttäjät eivät saa riittävästi tietoa tuotteiden ja palveluiden kyberturvallisuusominaisuuksista, jolloin luottamus erilaisiin digitaalisiin ratkaisuihin heikkenee (Kyberturvallisuusasetus, 2017, s. 24).

EU:n kyberturvallisuusviraston mukaan sertifiointijärjestelmässä käytettäisiin olemassa olevia standardeja teknisiin vaatimuksiin sekä arviointimenettelyjä niin, että virasto ei itse laatisi niitä (Kyberturvallisuusasetus, 2017, s.11). Standardit tukevat myös toisiaan, esimerkiksi ISO 27001-standardin läpäissyt organisaatio todennäköisesti läpäisee myös VAHTI 2/2010- ohjeen mukaisen auditoinnin ilman poikkeamia (Traficom, 2019). Brass ym., (2018, s. 4) toteavat ISO 27000 -sarjan tietoturvallisuuden hallintastandardin nousevan suosituimmaksi sovellettaessa sitä IoT-laitteita sisältävien järjestelmien arvioinnissa.

2.1.2 ISO 27001 -standardi

ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) muodostavat maailmanlaajuisen standardointiin erikoistuneen järjestelmän ja kansainvälisiä standardeja laaditaan ISOn ja IEC:n yhteisiä sääntöjä noudattaen. Kansainvälisen standardin hyväksyttyyn julkaisuun vaaditaan vähintään 75 % äänestäneistä

kansallisista jäsenjärjestöistä. (SFS-EN ISO/IEC 27001/2017, s. 4) CEN on hyväksynyt ISO/IEC 27001:2017 standardin sellaisenaan eurooppalaiseksi standardiksi (SFS-EN ISO/IEC 27001/2017, s. 3).

ISO 27001 kansainvälisessä standardissa esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä sekä jatkuvaa parantamista koskevia vaatimuksia (SFS-EN ISO/IEC 27001/2017, s. 5). Standardissa todetaan, että tietoturvallisuuden hallintajärjestelmän käyttöönotto organisaatiossa on strateginen päätös ja perustuu vapaaehtoisuuteen (SFS-EN ISO/IEC 27001/2017, s. 5).

Tietoturvallisuuden hallintajärjestelmä (ISO 27001) suojaa tiedon luottamuksellisuutta, eheyttä ja saatavuutta riskienhallinnan avulla ja näin vahvistaa eri sidosryhmien luottamusta asianmukaiseen riskienhallintaan kohde organisaatiossa, sitä voivat käyttää niin ulkoiset kuin sisäiset sidosryhmät (SFS-EN ISO /IEC 27001/2017, s. 5). Tietoturvallisuuden hallintajärjestelmä on osa organisaation prosesseja, joka liittyvät tärkeällä tavalla organisaation muihin prosesseihin, sekä yleisiin johtamis- ja hallintarakenteisiin (SFS-EN ISO/IEC 27001/2017, s. 5).

Tämä kansainvälinen standardi (ISO 27001:2017) on yhteensopiva muihin hallintajärjestelmästandardeihin liitteen SL mukaisesti, joka mahdollistaa hyödyn organisaatioille, jotka haluavat johtamisjärjestelmänsä täyttävän kahden tai useamman hallintajärjestelmästandardin vaatimuksia (SFS-EN ISO/IEC 27001/2017, s. 5).

ISO 27001:2017 sisältää myös vaatimuksia eri organisaatioiden käyttöön ja tarpeisiin mukautettua tietoturvariskien arviointia sekä käsittelyä. Vaatimukset ovat yleisluontoisia ja ne soveltuvat kaikille organisaatioille. (SFS-EN ISO/IEC 27001/2017, s. 5) Organisaation ilmoitettua noudattavansa kansainvälisen standardin (ISO 27001:2017) vaatimuksia, sen on noudatettava kaikkia 4–10 kohdissa mainittuja vaatimuksia (SFS-EN ISO/IEC 27001/2017, s. 5).

ISO 27001:2017 kansainvälisessä standardissa on lisäksi hallintatavoitteiden ja -keinojen viiteluettelo, jotka organisaation tulee täyttää. Standardi sisältää velvoittavat A.1 mukaiset hallintatavoitteet- ja keinot viiteluettelossa (SFS-EN ISO/IEC 27001/2017, s. 15). A-LIITE

2.2 IoT-alustat

IoT- alusta rakentaa yhteisen ekosysteemin laitteiden sekä pilvipalvelujen välille. Se mahdollistaa datan siirtämisen erilaisista IoT- laitteista suoraan palvelualustalle käyttöön. Varsinainen niin sanottu pääalusta voi jatkojalostaa saatua dataa ja jakaa sitä erilaisten analysointipalveluiden kautta rikastaen saatua tietoa lisää. (Toivanen, 2017, s. 4) Koska IoT-alustat käsittelevät ja sisältävät valtavan määrän dataa ja laitteita sekä niiden tietoja, monet tietoturvaan ja riskienhallintaan liittyvät asiat nousevat esille IoT-ympäristön ylläpidossa (Riahi ym., 2014, s. 1). Ylläpidon näkökulmasta IoT-pilvipalvelujen jatkuvana haasteena onkin ylläpitää riittävää tietoturvatasoa esimerkiksi standardisointien osalta ja taata IoT-alustojen luottamuksellisuus, eheys ja saavutettavuus. (Singh ym., 2016, ss. 2, 4)

Sicari ym. (2018, s. 1) toteavat IoT:n laajentuneen markkinoille tulleiden älykkäiden laitteiden ansiosta. Pilvipalveluun voidaan sijoittaa langattomia sensoreita ja käyttölaitteita, jotka mahdollistavat tiedonhankinnan eri verkkoympäristöistä (Sicari ym., 2018 s. 1). Myös Riahi ym. (2014, s. 1) toteavat IoT-laitteiden vuorovaikuttavan keskenään hyvin monialaisesti, jolloin törmätään erilaisiin turvallisuustekniikoihin sekä turvallisuuspoliitikkojen vaatimuksiin. Erilaisilla antureilla, valvottavilla laitteilla, ajoneuvoilla ja sensoreilla on mahdollisuus muodostaa yhteys internetin kautta. (Hejazi, ym., 2018)

2.2.1 IoT-alustojen haasteet

Monien tutkimuksien mukaan yrityksen vaikein tehtävä on valita sopiva IoT-alusta, jolla toimia, koska IoT-laitteet voivat parhaimmillaan tai pahimmillaan koostua useista eri toimittajien ja palveluntuottajien tuotteista (Hejazi ym., 2018). Atlam ja Wills (2019, s. 123) toteavat, että IoT-alustoihin liittyy myös erilaisten halpa-antureiden uhka. He näkevät, että tällaisilla halpa-antureilla IoT mahdollistaa erilaisten laitteiden ja esineiden olevan tunnistettavissa sekä paikannettavissa. Atlam ja Wills (2019, s. 123) jatkavat edelleen, että vaikka edellä mainitulla tavalla saavutetaan äärettömiä etuja, tuo se myös samalla uusia haasteita erityisesti turvallisuudessa ja yksityisyydessä.

IoT-alustat tallentavat, lähettävät ja jakavat tietoa eri yhteistyötahoille, jota käyttäjät ovat tallentaneet alustoille käyttäessään palveluita. Tällaiset tiedot voivat sisältää arkaluontoisia

tietoja, kuten liikesalaisuuksia tai muuta salassa pidettävää tietoa käyttäjästä. (Sicari ym., 2018, s. 16) Erilaisten IoT-alustojen toimintamallien seurauksena on, että käyttäjien on luotettava näihin palveluntarjoajan järjestelmiin sekä näiden tapaan hoitaa asioita, joilla käyttäjien erilaisia tietojansa käsitellään. Toinen vaihtoehto on, että käyttäjät eivät käytä kyseisen palvelun tarjoajan palveluita. (Sicari ym., 2018, s. 16)

Kun käytössä on satoja tai tuhansia erilaisia IoT-laitteita yhdellä toimijalla, on tärkeää, että sensoritietoja voidaan hallita ja seurata tehokkaasti. Tämä mahdollistaa samalla erilaisia automaattisia toimintoja IoT-laitteista saatavan datan avulla. (Toivanen, 2017, s. 5) Kun laitteiden määrä nousee IoT-alustoilla, verkkojen hallinnointi ja turvaaminen asianmukaisesti nousee palveluntuottajien haasteeksi (Singh ym., 2016, s. 2). Botta ym. (2015, s. 695) tuovat esille pilvialustojen ja IoT:n rajapintojen muodostavan epästandardisen heterogeenisen rajapinnan toimivuusongelmat. Heidän näkemyksensä mukaan, tällä hetkellä suurin osa IoT-laitteista on kytketty pilvialustoihin erilaisten verkkorajapintojen kautta. IoT-laitteita ei ole nimenomaisesti suunniteltu tehokkaaseen koneiden väliseen viestintään, joka johtuu verkon yleiskustannuksista, verkon viiveistä ja erilaisista tietojenkäsittelyistä johtuvista syistä (Botta ym., 2015, s. 695).

2.2.2 IoT-alustojen mahdollisuudet

Tulevien vuosien aikana IoT on yrityksille keskeinen tekijä digitalisaation muutoksessa. Yritykset hyödyntävät digitaalisella osaamisella erilaisia muutoksia liiketoimintamalleissa ja ekosysteemeissä. (MacGillivray, 2016, s. 2) IoT on kriittinen osa muutoksessa, koska IoT luo uusia liiketoimintamalleja ja mahdollistaa muutokset työprosesseissa sekä tuottavuuden parantamisessa (MacGillivray, 2016, s. 2). Nurse ym. (2018, s. 1) toteavat myös IoT:n tuottavan huomattavaa tuottavuuden kasvua, sekä lisäävän tehokkuutta niin teollisuudessa kuin maataloudessa. Radanliev ym., (2018a, s. 1) näkevät, että IoT-teknologia yleistyy kovaa vauhtia ja laajasti erilaisissa järjestelmissä ja järjestelmien osissa. He jatkavat, että IoT viittaa verkkoon liitettyihin laitteisiin, jotka voivat kommunikoida ja jakaa tietoja erilaisissa ympäristöissä.

Viime aikoina IoT-alusta on saanut huomattavan paljon huomiota liiketoiminnan arvon tuottamisessa epäsuorasti, koska IoT-alusta linkittää IoT-päätepisteet sovelluksiin sekä

tarvittavaan analytiikkaan (MacGillivray, 2016, s. 2). IoT-alustat mahdollistavat uusia ennen tuntemattomia liiketoimintamalleja kustannusten hajauttamisessa, joissa IoT:llä tehdään uusia palvelumalleja, kuten esimerkiksi valaistuspalvelu (LaaS) tai hissit kiinteistöön palveluna (Eaas) (Banafa, 2018).

Singh ym. (2016, ss. 3–4) luettelevat asioita, jotka tukevat pilvipalveluiden hyödyntämistä IoT-ympäristössä; pilvipalvelut ovat aina päällä ja globaalisti saavutettavissa, toiseksi pilvipalvelut ovat nopeasti skaalautuvia ja kolmanneksi pilvipalvelut auttavat hallitsemaan resursseja. Radanliev ym. (2019) toteavat myös IoT:n tarjoavan edistyneitä viestintämahdollisuutta koneiden välillä, erilaisilla protokollilla, verkkotunnuksilla ja sovelluksilla.

Radanliev ym. (2019a, s. 1) ovat tutkimuksessaan tulleet siihen johtopäätökseen, että IoT antaa yrityksille mahdollisuuden voittojen maksimointiin datan avulla, mutta myös tuovan uudentyyppisiä kyberriskejä sekä tietosuojakysymyksiä.

2.3 Tietoturva

Teknologia lisääntyy yhä enemmän modernissa yhteiskunnassa. Tärkeämmäksi asiaksi nousevat järjestelmien käyttöön liittyvät turvallisuus- ja luottamuskysymykset. (Nurse ym., 2017). Radanliev ym. (2018a, 1) toteavat IoT:n viittavan verkkoon liitettyihin laitteisiin, jossa IoT-laitteet jakavat ja kommunikoivat tietoja erilaisissa ympäristössä. He toteavat näiden lisäävän vakavasti turvallisuusriskiä sekä eettisiä huolenaiheita, joita organisaatioiden pitäisi ymmärtää käyttäessään IoT-ympäristöjä.

Viimeaikojen lisääntyneet tietoverkkohyökkäykset ovat osoittaneet kriittisten järjestelmien ja niihin liittyvien infrastruktuurin lisääntyneistä uhkista. Järjestelmiin kohdistuviin uhkiin on kiinnitetty huomiota lisäämällä uusia riskienhallinnan säännöksiä ja määräyksiä. (Gisladottir ym., 2016, s. 1644) Kun innovoidaan uusia liiketoimintamahdollisuuksia IoT-ympäristöön, on datan luotettavuus ja oikeellisuus erittäin tärkeää (PwC Suomi, 2016). Kaikenlaisissa IT-ympäristöissä tietomurron riski on laitteesta- tai järjestelmästä riippumatta olemassa, jos käytettävä ympäristö ei ole asianmukaisesti suojattu (PwC Suomi, 2016). Tietomurtojen aiheuttaessa potentiaalisia vakavia häiriöitä järjestelmille, niiden suorien vaikutusten lisäksi

aiheutuu merkittävää haittaa laitteiden jatkotarkastuksista ja vikaantuneiden laitteiden uusimisesta (PwC Suomi, 2016).

2.3.1 Tietoturvan uhkat

Tyypillisesti teknologia-alan startupit ja sijoittajat eivät kiinnitä huomiota tuotteidensa turvallisuuteen, vaan heidän ensisijainen tarkoituksensa on saada tuote mahdollisimman nopeasti markkinoille myyntiin (König ym., 2017, s. 29). Radanlievin ym. (2019) mukaan IoT-alustoihin liittyvät uudet teknologiat lisäävät yritysten tuottavuutta. He jatkavat, että teknologiat sisältävät kuitenkin liiketaloudellisen riskin altistua erilaisille teknisille, eettisille, turvallisuuteen ja yksityiseen liittyville riskeille.

König ym. (2017, s. 29.) ottavat kantaa myös asiakaspuolen ongelmiin, jotka johtuvat erilaisista kompromisseista tuotteiden käytettävyydessä ja turvallisuuden välillä. Näitä ovat muun muassa laitteiden oletuskäyttäjätunnukset ja salasanat. Tällaisia uhkia voi aiheutua esimerkiksi, jos järjestelmästä puuttuu sisäänkirjautumisen pakotettu vaihtaminen tai vaatimukset salasanan vaatimuksista (König ym., 2017, s. 29).

IoT-järjestelmät ovat luonteeltaan dynaamisia järjestelmiä, joissa jokainen huonosti suunniteltu IoT-laite voi häiritä koko järjestelmän turvallisuutta ja luotettavuutta, koska järjestelmät kytketään yhteen ketjuiksi (Atlam & Wills, 2019, s. 129). IoT-laitteiden helppo kytkeminen järjestelmään avaa vakavan turvallisuus uhkan, joka liittyy heterogeenisten laitteiden laajaan jakeluun ja niiden kykyyn muodostaa erilaisia yhteyksiä niistä erikseen ilmoittamatta tai lupia pyytämättä (Atlam & Wills, 2019, s. 129).

König ym. (2017, s. 29) mainitsevat mahdollisen kyberhyökkäyksen aiheuttavan kohteelle vakavia turvallisuusriskejä, joka voi johtaa pahimmillaan suuria taloudellisia ja tuotannollisia ongelmia automatisoidussa teollisuustuotannossa tai kokoonpanossa. Kuten Oorschot ja Smith (2019, s. 7) kuvaavat tilanteita, joissa IoT-laitteiden toimimattomuudella on välittömiä vaikutuksia ihmisten päivittäisessä toiminnassa, kuten rakennuksissa ja niiden lukituksissa, lämmitys- ja jäähdytysjärjestelmien hallinnassa, ajoneuvojen ohjaamisessa sekä lääkinnällisissä laitteissa, joiden vioittuminen suoraan vaikuttaa fyysisen maailman turvallisuuteen. Turvallisuuteen liittyvillä ongelmilla on IoT:n digitaalimaailmassa

suuremmat suorat vaikutukset fyysiseen turvallisuuteen, koska IoT-laitteet lisäävät laiteympäristön riskejä (Oorschot & Smith, 2019, s. 7).

2.3.2 Tietoturvan haasteet

Tietoturva tulee suunnitella aina riskiperusteisesti suunnitteluvaiheesta toteutus- ja seurantavaiheeseen asti (Jha & Sunic, 2014). Riskipohjainen ajattelu alkaa komponenttien erilaisten arvojen määrityksistä ja tunnistamisesta, näin tunnistetaan myös sellaiset kohteet, joita ei voida suojata tehokkaasti (Jha & Sunic, 2014).

Erilaiset IoT-järjestelmät voivat sisältää miljardeja heterogeenisia laitteita, jotka aiheuttavat verkon hallinnan näkökulmasta suuren ongelman ja tekee IoT-järjestelmästä erittäin vaikeasti hallittavan (Atlam & Wills, 2019, s. 137). IoT-laitteita käyttöönotettaessa, turvallisuushaasteet tulee priorisoida, jotta käyttäjät olisivat varmoja IoT-laitteisiin liittyvien sovellusten turvallisuudesta (Atlam & Wills, 2019, s. 129).

Atlam ja Wills (2019, s. 137) näkevät, että IoT-järjestelmän monimuotoisuuden vuoksi, verkon kaikkien laitteiden turvallisuudenhallinta on vaikeasti hallittavissa oleva toimenpide. IoT-järjestelmän sovellusten kehittämissä on huomioitava uusia turvallisuuteen ja luotettavuuden liittyviä suunnittelutapoja (Atlam & Wills, 2019, s. 141). Jha ja Sunil (2014) myös mainitsevan IoT:n tuovan laitteille aivan uuden ulottuvuuden manipuloinnin osalta, joilla voi olla tuhoisat vaikutukset järjestelmään tai yleiseen ympäristöön, kuten turvallisuuteen ja tuottavuuteen.

Ziegler ym. (2017) tuovat esiin rakennusten kyberfyysisten järjestelmien ja verkkojen haavoittuvuuksien lisääntymisen. Ongelmat johtuvat suurista, monimutkaisista, hajautetuista sekä toisistaan riippuvaisista älykkäistä heterogeenisista IoT- järjestelmän osista. Tällaisessa tilanteessa tietoturvan järjestelmävalvojalla pitää olla syvällinen ymmärrys kokonaisuudesta. (Ziegler ym., 2017)

2.3.3 Tietoturvan tavoitteet

Kyberturvallisuus tunnistetaan kansallisesti kriittisenä ja poliittisena kysymyksenä monissa maissa. Verkkoriskien taloudelliset vaikutukset ja tietoturvan merkitys kasvaa, kun IoT-laitteiden integrointi lisääntyy edelleen tuotteiden valmistuksessa, logistiikassa, kaupungeissa, liikenteessä, sähköverkoissa mukaan lukien rahoitusmaailman toimet sekä, erilaisissa lääkinnällisissä laitteissa ja järjestelmissä. (Radanliev ym., 2018)

IoT-sovelluslaitteiden ja erilaisten järjestelmien yleistyminen riippuu Sicarin ym. (2018, s. 1) mukaan tietoturvan tasosta. Miten loppukäyttäjä luottaa järjestelmän turvallisuuteen, jossa käyttäjien tietoja hallinnoidaan kolmen tietoturvan peruskäsitteen (luottamuksellisuus, eheys ja saatavuus) avulla sekä yksityisyysvaatimuksilla. Nämä keskeiset käsitteet on avattu luvussa 1.4.

Tietoturva mahdollistaa yrityksen liiketoiminnalle läpinäkyvän, turvallisen sekä taustalla toimivan toiminnan, joilla yritys antaa kohtuullisen varmuuden loppuasiakkaille, että heidän etunsa on suojattu mahdollisilta uhilta (Jha & Sunil, 2014).

IoT-laitteita sisältävien järjestelmien yksi tärkeimmistä prioriteeteista on turvallisuus. Sen avulla voidaan estää IoT-järjestelmän ja sen sisältämien erilaisten elementtien aiheuttamat fyysiset vauriot sekä ei-toivotut uhkat ja haittavaikutukset, jotka uhkaavat järjestelmää sen ympäristössä sisä- ja ulkopuolelta. (Atlam & Wills, 2019, s. 141)

Monet IoT:n näkökohdat ovat usein kuluttajalähtöisiä, jolloin ihmisten tai yritysten on hyväksyttävä IoT- teknologioiden uudet ominaisuudet, joissa tiedoilla maksetaan palvelun tai tuotteen käytöstä. Järjestelmien ja laitteiden on oltava luottamuksellisia sekä turvallisia käyttää. (Pasquier ym. 2017, s. 334)

2.4 Riskienhallinta

Riskienhallintaprosessi on yleisesti vaikea prosessi ja erityisen vaikean siitä tekee IoT-riskien arvioiminen. Tämä tulee esiin käytettäessä perinteisiä riskienhallinnan menetelmiä, koska ne eivät pysty ottamaan huomioon IoT:n erilaisia vivahteita. (Nurse ym., 2018, s. 2) Turvallisuus- ja luottamuksenhallinnan näkökulmasta tarkasteltuna, haasteeksi nousevat olemassa olevien

riskienarviointimenetelmien rakentaminen ennen IoT-pilvipalvelujen käyttöönottamista, eivätkä ne enää välttämättä vastaa automatisoitujen järjestelmien monimutkaisuuteen (Nurse ym., 2017, s. 1).

Nurse ym. (2018, s. 1) toteavat tutkimuksessaan IoT-teknologiajärjestelmien monimutkaisuuden, yleisyyden ja jatkuvasti kasvavan automaation tuovan tietoturvahaasteita. Erityisesti IoT:n käytössä tarvitaan riskien arviointiin uusia lähestymistapoja, joilla varmistetaan järjestelmän luottamuksellinen rakentaminen (Nurse ym., 2018, s. 1). Nurse ym. (2017, s. 2) toteavat riskienarviointiprosessissa tärkeänä lähtökohtana uhkan lähteen tunnistamisen eli juurisyyn, josta tapahtuma on saanut alkunsa. Niinkään tärkeää ei ole tunnistaa uhkaa, niiden haittoja tai kriittisiä ominaisuuksia. Aina on myös mahdollista, että riskienhallinnassa ei tunnisteta tai havaita riskiä, joka myöhemmin realisoituu. (Nurse ym., 2017, s. 5)

Huomionarvoinen asia on myös, että riskienarviointia käytetään toipumissuunnitteluun ja riskivaikutusten arviointia päätöksenteossa tietoverkkoriskeihin liittyvissä asioissa (Radanliev ym., 2020) Myös Gisladottir ym. (2016, s. 1644) mainitsevat riskienhallintakäytäntöjen laajasta sovellettavuudesta useilla eri aloilla ohjelmistojen ja laitteiden suunnittelussa sekä käytössä. Riskienarvioinnit tapahtuvat käyttämällä alan kehittämiä arvostettuja menetelmiä kuten ISO 27000-sarjan standardit, NIST (National Institute of Standards and Technology) erikoisjulkaisut sekä muita alan standardeja (Nurse ym., 2018, s. 1)

2.4.1 Riskienhallinnan haasteet

Nykypäivän kriittiseen IoT-järjestelmien käyttöönottoon liittyviä riskejä ei huomioida monimutkaisissa infrastruktuurijärjestelmissä, jotka ovat paljon monimutkaisempia ja mahdollistavat samalla riskienhallinnan epäonnistumisen (Radanliev ym. 2018). Nurse ym., (2017, s. 1) tuovat esiin saman näkökulman, jossa uusista ekosysteemeistä esiin nousevat riskit voivat vaikuttaa negatiivisesti riskien käsittelyyn ja arviointiin vanhoilla menetelmillä. He jatkavat näkemyksellään tietoverkkohyökkäyksistä, jotka voivat vaikuttaa myös sosiaalisiin prosesseihin, joilla on vaikutusta koko väestöön reaaliajassa (Nurse ym., 2017, s. 1).

IoT perustuu erilaisiin älykkäisiin laitteisiin kyberfyysisessä ympäristössä toimivien koneiden ja järjestelmien välillä. Näistä rakentuu järjestelmiä, jotka pystyvät toimimaan vuorovaikutuksessa todellisen toimintaympäristön kanssa sekä luovat uusia riskejä vähemmän suojattujen laitteiden integroituessa edelleen toisiin. (Radanliev ym., 2020) Myös Nurse ym. (2017, s. 2) viittaavat kyberriskin muodostuvan edellisten käsitteiden yhdistelmistä, jossa hyökkäyksen tai haavoittuvuuden uhka ja todennäköisyyden toteutuminen tuottaa yritykselle vahinkoa.

IoT-laitteita sisältävien järjestelmien riskienhallinnassa uhkien ja haavoittuvuuksien selkeä tunnistaminen on avain onnistumiseen. Tietoturvasertifiointimenetelmien tulisi olla kustannustehokkaita ja menetelmien olisi vastattava IoT-markkinoiden liiketoiminnan vaatimuksiin sekä tarpeisiin. (Matheu-Garcia ym., 2018, s. 1)

IoT-järjestelmien heterogeenisyys vaikeuttaa myös sertifioitujen laitteiden ja järjestelmien vertailua, koska sertifioinnit on tehty erilaisilla sertifiointimenetelmillä eri maissa. Ne on yleensä rakennettu erilaisten vaatimusten sekä yhteneväisten arviointiratkaisujen puutteiden vuoksi. (Matheu-Garcia ym., 2018, s. 3) IoT:n yksi suurimmista vaikeuksista riskienhallinnassa on, että IoT-teknologia kehittyy nopeammin kuin muu ympäröivä teknologia, tämä aiheuttaa ongelmia eri maiden kykyyn muodostaa yhteisiä normeja ja turvallisuusmääräyksiä (Radanliev ym., 2019).

Radanlievin ym. (2020) mukaan tietoverkkoriskien vähentämiseen liittyviä IoT-laitteiden elinkaariprosessin riskejä tulee tarkastella säännöllisillä aikaväleillä. Näihin liittyvien riskien vähentäminen edellyttää myös tietojen, prosessien, laitteiden ja järjestelmien kokoamista riskienhallinnan kokonaisuuteen (Radanliev ym., 2020).

2.4.2 Riskienhallinnan hyödyt

Hyvä turvallisuuskulttuuri on ensiarvoisen tärkeää, arvioitaessa järjestelmään kohdistuvia erilaisia riskejä. Turvallisuuskulttuuri korostuu käytettäessä nykypäivän järjestelmiä ja erityisesti, kun puhutaan erilaisten järjestelmien yhteenliitettävyydestä. (Nurse ym., 2018, s. 5) Myös Atlamin ja Willsin (2019, s. 123) mukaan IoT- tuotteiden ja palveluiden

turvallisuuden sekä yksityisyyden varmistaminen on oltava keskeinen painopiste IoT-ekosysteemissä, jolloin käyttäjät voivat luottaa IoT-laitteisiin ja niihin liittyviin palveluihin.

Nursen ym. (2017, s. 6) näkemyksen mukaan, suuri määrä laitteita ja toimijoita muodostavat suuren osan nykyisestä sekä tulevasta IoT-ympäristöstä, nämä muodostavat laajan joukon erilaisia yhteyksiä. Pelkästään protokollat ja viestintästandardit eivät kuitenkaan riitä pitämään yhteyksiä yllä, vaan tarvitaan eri toimijoiden välistä monitasoista yhteistyötä. Yhteistyössä korostuu datan käsittely ja sen vastaanoton toimintamallit. Yhteisten toimintamallien rakentaminen lisää organisaation vaikuttavuutta yhteistyökumppaneihin nähden. (Nurse ym., 2017, s. 6)

IoT:n riskienarviointia on tehtävä koko toimitusketjussa yhdessä mahdollisten yhteistyökumppaneiden kanssa, tällä saavutetaan dynaamisempi taloudenkehitys koko toimitusketjussa (Nurse ym., 2018, s. 6). Nurse ym. (2018, s. 7) näkevät ratkaisuna erilaisten IoT-järjestelmien riskienhallinnassa mahdollisuuden jakaa riskejä eri kumppanuusyritysten välillä, jossa laajennettu valvonta ja luottamus perustuu tiiviiseen yhteistyöhön. Kattava riskienarvioinnin yhteistyö eri toimijoiden kesken parantaa kokonaisnäkemystä IoT-järjestelmästä, sekä mahdollistaa yritysten välisen arvion yhteisistä riskeistä ja tukee tarvittaessa resurssien tehokasta käyttöä (Nurse ym., 2018, s. 7).

Riskipohjaisella mukautuvalla arvioinnilla kyetään ennustamaan jatkuvasti muuttuvassa IoT-ympäristössä järjestelmiin kohdistuvia aiemmin määrittelemättömiä ongelmia ja vaikutuksia, toteuttamaan suunnitellut toimet, vähentämään riskejä sekä riskialtistusta (Radanliev ym., 2018b, s. 15).

2.5 Auditointi

Auditoinnissa esiin tulevat muutokset voivat johtua uusien tietoturva-aukkojen havaitsemisesta, tunkeutumishyökkäyksistä tietoturva-aukkojen hyödyntämisessä, erilaisissa päivityksistä, korjaustiedostoista tai laitteen ympäristön muutoksista (Matheu-Garcia ym., 2018, s. 16).

Kansainvälinen standardisointijärjestö (ISO) on tehnyt kymmenen viimeisen vuoden aikana monia tutkimuksia ja yrittänyt selvittää standardoinnista aiheutuvia taloudellisten hyötyjen mahdollisuutta nopeasti kehittyvää teknologiaa käyttäville yrityksille. Ilman selkeitä suuntaviivoja IoT-laitteissa ja järjestelmissä, kuten asetuksia ja yleisiä standardeja, sääntelemättömät asiat vaikuttavat teollisuuden toimintaan haitallisesti. (Saleem ym., 2018)

IoT-järjestelmien verkkoturvallisuuteen on kiinnittänyt huomiota myös Brass ym. (2018, s. 4) omassa tutkimuksessaan ja vahvistaa hajanaisen standardoinnin maailman IoT:n tietoturvan osalta. Samaan näkemykseen ovat tulleet myös Saleem ym. (2018) joiden mukaan IoT:n kehitystä rajoittaa puutteellinen sääntely alalla. Saman johtopäätöksen on tehnyt myös Euroopan parlamentin neuvosto kyberturvallisuusasetuksessa, jossa todetaan tieto- ja viestintätekniikan kyberturvallisuussertifioinnin tilanne tällä hetkellä melko heikoksi (Kyberturvallisuusasetus, 2017, s. 10). Kesäkuussa 2019 tuli voimaan EU:n Kyberturvallisuusasetus, joka tulee todennäköisesti kasvattamaan Euroopassa entisestään sertifiointien kysyntää sekä käyttöä. (Traficom, 2019, s. 3)

2.5.1 Auditoinnissa havaitut haasteet

Auditointi eli niin sanottu varmennusprosessi on ihmiskeskeinen prosessi, jossa arvioija arvioi hallintajärjestelmän toimintaa tarkastuksen aikana. Kaikki muutokset käyttöönoton jälkeen voi laukaista uudelleensertifioinnin tarpeen, joka on usein kallis prosessi auditoinnin kohteena olevalle yritykselle. (Singh ym., 2016, s. 10) Singh ym. (2016, s. 11) mainitsevat myös tärkeänä tarkastusmekanismien kehittämisen IoT- järjestelmissä, jotta huomioidaan ja varmistetaan kaikki asiaankuuluvat näkökohdat. Heterogeeniset tekniikat ovat IoT-järjestelmille Sicarin ym. (2014, s. 146) mukaan ominaisia, koska ne sopivat innovatiivisten palvelujen tarjoamiseen eri sovellusalustoilla ja tämän takia turvallisuus- ja yksityisyydensuojavaatimuksilla on keskeinen rooli järjestelmissä.

Myös Radanliev ym. (2018) viittaavat uuden tyyppisten teknologioiden aiheuttavan enemmän uusia riskejä, joiden ennakointiin nykyisiä arviointi- ja hallintajärjestelmiä ei ole suunniteltu. Myös Nurse ym. (2018, s. 1) näkevät asian samalla tavalla ja toteavat, että nykyiset turvallisuusjärjestelmät eivät sovellu säännöllisten turvallisuusarviointien tekemiseen, koska erilaisten IoT- laitteita sisältävien järjestelmien rajapintoja ei tunneta

tarpeeksi hyvin järjestelmien turvallisuusarvioinnin aikana. Nurse ym. (2018, s. 2) lisäävät turvallisuuden, yksityisyyden ja luottamuksen olevan keskeisiä huolenaiheita IoT-järjestelmissä, lisäksi niissä on monia ratkaisemattomia haasteita turvallisuuden saavuttamiseksi.

Gisladottir ym. (2016, s. 1645) mainitsevat osaltaan liian rajoittavan sääntelyn johtavan ihmisten kykyyn suorittaa työssään vaadittuja turvallisuusvaatimuksia, tämä johtuu ihmisten kyvystä kiertää tai suoraan jättää huomioimatta vaadittuja säädöksiä. Heidän mukaansa tiukempi sääntely vähentää ulkoisiin uhkiin liittyviä riskejä, mutta lisää riskiä sääntöjen täytäntöönpanoon johtavien inhimillisten tekijöiden vuoksi (Gisladottir ym., 2016, s. 1645).

2.5.2 Tietoturva-auditoinnin hyödyt

Myöhemmässä vaiheessa organisaatioon samalla standardilla tehdyt auditoinnit voivat mahdollistaa jatkuvan seurannan ja toistettavuuden mittaamisen avulla (Saleem ym., 2018). Singh ym. (2016, s.10) mainitsevat, että sertifiointi on usein ainoa organisaation käytettävissä oleva tapa osoittaa tietoturvasäännösten noudattaminen.

ISO 27001-standardin noudattaminen vaikuttaa kiinnostavan tahoja myös vähemmän säännellyillä aloilla, jotka eivät normaalisti osoita noudattavan standardien vaatimuksia. (Singh ym., 2016, s. 10).

Luotettavat tietoturva-auditoinnit ovat merkityksellisiä pilvivuokralaiselle, loppukäyttäjille sekä palvelun tarjoajille. Eri vuokralaiset ja palvelun käyttäjät voivat olla varmoja siitä, että tuotettu palvelu- tai erilaiset palvelualustat toimivat tietoturva-asiat huomioiden. (Singh ym. 2016, s.11) Tietoturva-auditoinnilla on merkitystä myös lakien ja asetuksien noudattamisen todentamisessa tarkastusten yhteydessä, jolla voidaan osoittaa tietoturva-asioiden toiminnan asianmukaisuus (Singh ym., 2016, s. 11).

Tietoturva-auditointeja käytetään myös havaitsemaan sekä todentamaan odotetut ja odottamattomat suojaustason muutokset, joissa IoT-laitteen tai laitteiden haavoittuvuuksia arvioidaan valvottavan hallintajärjestelmän avulla. Samalla arvioidaan, onko haavoittuvuus sovellettavissa valvottavaan kohteeseen. (Mathea-Garcia ym., 2018, s.17) Seuranta-auditoinnissa ja uudelleen tarkastelussa voidaan havaita uusia haavoittuvuuksia, nämä uudet

tapahtumat voidaan sisällyttää turvallisuusriskien arviointiin, jotka käynnistävät tapahtuman uudelleen arvioinnin sekä johtavat tapahtuman hallittuun suojaustason saavuttamiseen (Mathea-Garcia ym., 2018, s. 17).

Vaikka hallintajärjestelmän kehittämisestä muodostuu kustannuksia, on auditoitavan järjestelmän kehittämisestä aiheutuneet kustannukset kuitenkin huomattavasti suuremmat kuin sertifioinnista aiheutuneet kustannukset (Traficom, 2019).

3 Tutkimuksen kuvaukset ja menetelmät

Tässä luvussa esitellään tämän opinnäytetyön tutkimusasetelma sekä perustellaan menetelmävalinta. Edellisen lisäksi esitellään, miten tutkimusaineisto on kerätty ja haastateltavat on valittu. Lisäksi tarkastellaan aineiston luotettavuutta ja esitellään opinnäytetyön aineiston analysointiprosessi.

3.1 Tutkimusstrategia

Tämä opinnäytetyö toteutettiin tutkimuspainotteisena, kvalitatiivisena eli laadullisena tutkimuksena. Kvalitatiivisessa tutkimuksessa Hirsjärven ym. (2016, s. 161, 164) mukaan tutkittavaa kohdetta pyritään tutkimaan mahdollisimman kokonaisvaltaisesti, jossa korostuu tiedonhankinta ja aineiston kerääminen todellisissa tilanteissa. Kananen (2008, s. 56) toteaa osaltaan, että tiedonkeruu ja analyysivaihe kytkeytyvät tiiviisti yhteen prosessin aikana. Koska laadullisessa tutkimuksessa Kanasen (2008, s. 57) mukaan aineisto ohjaa aina tutkimusta, voidaan puhua aineistolähtöisestä tutkimuksesta.

> ”Syklisyys ja jatkuva reflektointi kuuluvat tämän tutkimusotteen piirteisiin ja tutkimuksen validiteetti- eli pätevyyskysymyksiin” (Kananen, 2008, s.57).

Kananen (2010, s. 37) nostaa esiin myös ilmiön tunnistamisen tärkeyden laadullisessa tutkimuksessa. Hänen näkemyksensä mukaan, laadullista tutkimusta käytetään, jos ilmiötä ei tunnisteta.

Tutkimuksessa käsiteltiin virallisten akkretoitujen organisaatioiden asiantuntijoiden näkemyksiä ISO 27001-standardin soveltumisesta IoT-laitteita sisältävien alustojen hallintajärjestelmien arviointiin ja standardin vaatimusten soveltuvuutta IoT-alustojen nopeasti muuttuviin riskeihin. Aihetta tutkittiin myös auditoinnin tilaavien yritysten näkökulmasta. Tutkimukseen osallistettiin myös yritysten IoT-asiantuntijoita, joiden roolina oli arvioida ISO 27001-standardin ominaisuuksien soveltuvuutta IoT-laitteita sisältävien järjestelmien hallintajärjestelmissä.

Aihealuetta lähestytään laajemmasta näkökulmasta, siirtyen yksityiskohtaisempaan tietoon. Tämä tukee laadullisen tutkimuksen käyttämistä tässä opinnäytetyössä.

> Kanasen (2008, s. 57) mukaan laadullisessa tutkimuksessa toteutuu laadullisen tutkimuksen prosessi, joka muistuttaa ”hermeneuttista kehää, jossa ilmiön kerroksellisuus kuoritaan sipulin tavoin lähestyen ydintä eli totuutta.”

3.2 Tiedonhankinnan strategia

Tiedonhankinnan strategiana tässä tutkimuksessa käytettiin tapaustutkimusta (case study). Tapaustutkimus voidaan määritellä empiiriseksi tutkimukseksi, jonka avulla hankitaan tietoja monipuolisesti ja monilla eri tavoilla. Sen avulla tutkitaan nykyajassa tapahtuvaa tapahtumaa sekä tietyssä ympäristössä toimivaa ihmistä. Tapaustutkimus voidaan ymmärtää keskeisenä kvalitatiivisen metodologian tiedonhankinnan strategiana. (Metsämuuronen, 2009, ss. 222, 224) Mills ja Birks (2014, ss. 145, 149) toteavat, että tapaustutkimusta käytetään monipuolisesti ja laajasti erityyppisten tieteenalojen tutkimusmenetelmänä. Heidän mukaansa, sen avulla vastataan erityyppisiin tutkimuskysymyksiin. Huomionarvoista on, että tapaustutkimuksessa ei ole oikeaa tai väärää lähestymistapaa tutkittavaan ongelmaan. (Mills & Birks, 2014, s. 149) Kananen (2008, ss. 84–85) mainitsee myös, että tapaustutkimuksessa voidaan tutkia vain yhtä tai vaihtoehtoisesti useampia tapahtumia, joiden tavoitteena on päästä syvälliseen yhden tapauksen ymmärtämiseen. Myös Metsämuuronen (2009, s. 223) tuo esiin näkemyksen, että tapaustutkimuksella pyritään kokoamaan monipuolisesti tietoa ja tavoitteena on ilmiön kokonaisvaltainen ymmärtäminen. Samalla tapausta pyritään luotaamaan syvälle ja analysoimaan ilmiötä (Metsämuuronen, 2009, s. 223).

Tutkittava tapaus voi olla laaja-alaisesti ajateltuna yritys tai yhteisö, mutta se voi olla kapea-alaisemmin myös ihmisryhmä tai yksilö. Tapaustutkimuksen tutkimusaineiston lähteinä toimivat esimerkiksi erilaiset tieteelliset dokumentit, arkistot, haastattelut sekä havainnot. (Kananen, 2008, s. 84) Tässä opinnäytetyössä hyödynnettiin laaja-alaisesti tieteellisiä artikkeleita sekä asiantuntijahaastatteluja.

3.3 Aineiston kerääminen

Tässä alaluvussa kuvataan opinnäytetyön tutkimuksen kerääminen ja haastattelujen toteutuksen eteneminen. Opinnäytetyön tekijä piti tutkimuspäiväkirjaa vuoden 2020 kesästä alkaen. Päiväkirjaan kirjattiin tutkimukseen liittyviä havaintoja sekä yksityiskohtia, jotka liittyivät esimerkiksi haastattelukysymysten rakentumiseen tai ideoihin, jotka nousivat esille aihealueen tutkimusartikkeleja luettaessa. Tutkimuspäiväkirjan ylläpitäminen jatkui läpi haastatteluiden. Tutkimuspäiväkirja on Hirsjärven ym. (2016, 45) mukaan tutkimuksen edistämisessä ja erilaisten tutkimukseen liittyvien yksityiskohtien merkitsemiseen erinomainen apuväline.

<u>Haastatteluihin valmistautuminen</u>

Haastattelukysymyksiä rakennettiin ja tarkennettiin koko teoriaosuuden rakentumisen ajan. Kysymyksiä reflektoitiin jatkuvasti tutkimuskysymyksiin. Alkuvaiheessa kysymyksiä oli noin 30–40 kappaletta, joista kysymysten määrä supistettiin 14:ään ydinkysymykseen. Nämä kysymykset jakaantuivat neljään eri pääaihealueeseen: lainsäädäntö, IoT-alustat, riskienhallinta ja tietoturva sekä auditointi.

Kysymyksiä testattiin testihaastattelun avulla, jonka perusteella muutettiin joitain kysymyksiä tai poistettiin kokonaan päällekkäisyyden vuoksi. Testihaastattelu suoritettiin kasvokkain haastateltavan yrityksen toimitiloissa lokakuun puolivälissä 2020. Haastattelu tallennettiin digitaaliseen tallentimeen. Samalla mitattiin haastattelun ajankäyttöä.

Oman haasteensa haastattelujen aikataulutukseen toi syksyllä ilmi tullut vakava tietomurto Suomessa toimivan yrityksen henkilötietoja sisältävään järjestelmään. Tämä lisäsi haastateltavien yritysten henkilöiden työkuormaa. Viimeinen haastattelu tehtiin juuri ennen

joulua 2020. Osa haastateltaviksi suunnitelluista henkilöistä kieltäytyivät työkiireisiinsä vedoten. Haastatteluja tehtiin kaikkiaan kuusi kappaletta, näistä neljä kappaletta tehtiin akkretoiduille sertifiointiyritysten asiantuntijoille ja kaksi kappaletta yritysmaailmaa edustaville tietoturva-asiantuntijoille. Myös Hirsjärvi ym. (2016, s. 179) toteavat, että haastateltavien määrään ei ole yksiselitteistä vastausta, vaan siihen vaikuttaa järkevä ajankäyttö sekä kohtuulliset kustannukset. Kvalitatiivisessa tutkimuksessa aineistona voi olla vain yhden henkilön haastattelu tai esimerkiksi vain yksi tapaus, koska tarkoituksena ei ole etsiä keskimääräisiä yhteyksiä, eikä tilastollisia säännönmukaisuuksia (Hirsjärvi ym., 2016, s. 181). Samaa mieltä on myös Kananen (2010, s.54) joka toteaa, että haastateltavien määrää ei etukäteen voida määritellä.

Haastateltavien valinta

Tutkimushaastattelua suunniteltaessa tutkijan on ensimmäisenä ratkaistava peruskysymykset: ketä, mitä, milloin ja missä haastattelut tehdään. Laadullisessa tutkimuksessa haastateltavat valitaan tiedon saannin näkökulmasta. (Kananen, 2008, ss. 75–76) Haastateltavat valittiin Suomessa toimivien virallisten akkretoitujen sertifiointiyritysten asiantuntijoista, joilla on vahva kokemus ja pitkä osaaminen ISO 27001 -standardin vaatimuksista. Haastateltavat valitaan siten, että tutkittava ilmiö liittyy heihin kiinteästi (Kananen, 2010, s. 54). Osaan akkretoitujen sertifiointiyritysten asiantuntijoista opinnäytetyön tekijällä oli jo aikaisemmasta työhistoriasta johtuvia yhteyksiä. Osa haastateltavista olivat ennestään tuntemattomia tutkimuksen tekijälle. Nämä henkilöt pyydettiin mukaan haastateltaviksi, jonkun toisen asiantuntijan suosituksen perusteella. Yritysmaailman molemmat tietoturva-asiantuntijat valikoituivat haastatteluun heidän monipuolisen IoT-asiantuntemuksensa vuoksi.

Haastateltavia lähestyttiin ensin puhelinsoitolla ja tiedusteltiin halukkuutta ottaa osaa haastatteluun. Haastateltavien kanssa sovittiin aikataulusta. Puhelimessa keskusteltiin aiheesta ja opinnäytetyön tekijä avasi aihetta potentiaalisille haastateltaville. Haastattelujen sopimisen jälkeen tutkimuksen tekijä lähetti välittömästi haastateltavilla omat yhteystietonsa. Tämä oli tärkeää luottamuksen rakentamisen näkökulmasta, erityisesti niiden haastateltavien osalta, joita tutkija ei ennestään tuntenut.

Haastattelukysymykset lähetettiin haastateltaville pari päivää ennen haastattelun toteutumista. Kysymykset lähetettiin sähköpostilla, näin haastateltavilla oli mahdollisuus valmistautua kysymyksiin etukäteen. Tutkimuksen tekijä näkee, että haastattelukysymysten etukäteen lähettäminen mahdollisti asiantuntijalle vastata syvällisemmin kysymyksiin. Haastattelutilanteessa vaikuttikin siltä, että kaikki olivat perehtyneet kysymyksiin etukäteen. Haastattelujen Teams-kutsut lähetettiin kysymysten kanssa samanaikaisesti.

Haastatteluiden toteutus

Tämä tutkimus toteutettiin puolistrukturoituna haastatteluna. Puolistrukturoidulle haastattelulle on ominaista, että muotoilu ja järjestys ovat kaikille haastateltaville samoja, mutta valmiita vastausvaihtoehtoja ei käytetä. Haastateltaville annetaan mahdollisuus vastata kysymyksiin omin sanoin. (Eskola & Suoranta, 2014, s. 87) Myös Kananen (2008, s. 73) kertoo, että puolistrukturoidussa haastattelusta puuttuvat vastausvaihtoehdot ja kysymykset esitetään avoimina. Puolistrukturoitu haastattelu sopii Metsämuurosen (2009, s. 247) mukaan tilanteisiin, joissa käsitellään arkoja aiheita tai halutaan selvittää heikosti tiedostettuja asioita. Onkin tärkeää, että asiaa kysytään kaikilta haastateltavilta samalla tavalla standardoidusti, jolloin saadaan näyte tietystä perusjoukosta (Hirsjärvi ym., 2016, s. 193).

Haastattelut toteutettiin Teams-haastatteluina, jolloin Hyvärisen ym. (2017, s. 271) näkemyksen mukaan voidaan pitkien etäisyyksien vuoksi toimia tehokkaasti ja säästää kustannuksia. Maantieteellinen etäisyys on yksi keskeisimmistä syistä, miksi laadullisissa tutkimuksissa tehdään etähaastatteluja (Ikonen, 2017, s. 271). Haastateltaville kerrottiin haastattelujen tallentamisesta jo siinä vaiheessa, kun haastatteluaikoja sovittiin puhelimessa. Teams-kokouksissa on mahdollista käyttää myös kameraa, mutta ensimmäisten haastattelujen aikana huomattiin ongelmia yhteydessä ja kameran käytöstä luovuttiin pian. Kameraa pidettiin kuitenkin päällä haastattelun alkuvaiheessa, kun osapuolet esittäytyivät toisilleen. Kameran käyttäminen haastattelun alussa lisäsi tutkimuksen tekijän mielestä molemminpuolista luottamusta. Teams-haastattelu taltioitui myös haastateltavan kalenteriin, josta hänellä oli mahdollisuus tarkistella vastauksiaan jälkeenpäin. Haastattelujen tallennus sujui ilman ongelmia ja tallenteiden avulla suoritettiin litterointi. Haastattelut kestivät noin tunnin, riippuen haastateltavan aikataulusta ja siitä, miten syvälle

haastattelija onnistui keskustelun viemään. Haastattelut toteutettiin anonyymisti. Tämä on tärkeä kriteeri yksityiselle sektorille haastatteluja tehtäessä. Haastateltavien asiantuntijoiden, eivätkä heidän edustamansa yritysten yksityiskohtaiset tiedot nouse esiin missään tutkimuksen vaiheessa. Haastateltavan tunnistetieto häivytetään ja korvataan pseudonimellä (Ranta & Kuula-Luumi, 2017, s. 419).

Kvalitatiivisen aineiston keräämisessä käytetään aineiston riittävyyteen liittyvää saturaation käsitettä. Tämä tarkoittaa, että haastatteluja tehdään niin paljon, että uudet tapaukset eivät tuota enää tutkimusongelman kannalta uutta tietoa (Hirsjärvi ym., 2016, s. 182; Eskola & Suoranta, 2014, s. 62) Hirsjärvi ym. (2016 s. 182) pitävät saturaation käsitettä kuitenkin ongelmallisena, kun tarkastellaan kvalitatiivisen tutkimuksen piirrettä, että kaikki tapaukset ovat ainutlaatuisia. Tässä tutkimuksessa voidaan todeta, että saturaatiopiste saavutettiin. Haastattelujen avulla saavutettiin käsitys akkrekoitujen virallisten auditoijien näkemyksistä ISO 27001 -standardin soveltuvuudesta IoT-järjestelmien auditoinnissa.

Haastattelujen litterointi

Haastatteluaineiston purkaminen tehtiin litteroimalla materiaali suoraan haastatteluista. Hirsjärven ja Hurmeen (2009, s. 138) mukaan litterointi voidaan tehdä koko haastattelusta tai suppeammin valikoiden tiettyjen teemojen osalta. Tässä tutkimuksessa materiaali litteroitiin kokonaisuudessaan erittäin tarkasti. Tosin Hirsjärven ja Hurmeen (2009, s. 139) näkökulman mukaan ei ole olemassa yksiselitteistä ohjetta aineiston litteroinnin tarkkuudesta.

Kananen (2008, s. 80) kannustaa mahdollisimman tarkkojen litteraatioiden tekemiseen, koska haastateltavien tarkkoja kommentteja ”voidaan käyttää sitaattina sellaisenaan myöhemmin lopullisessa raportissa”. Näin toimittiin myös tämän tutkimuksen osalta.

Haastattelututkimuksen tekstiksi puretut äänitallenteet muodostavat tutkimusaineiston (Ruusuvuori & Nikander, 2017, s. 427).

Tämän opinnäytetyön tekijä litteroi haastattelut itse mahdollisimman pian haastattelujen jälkeen. Haastattelut kestivät noin tunnin. Hirsjärven ja Hurmeen (2009, s. 140) näkemyksen mukaan yhden tunnin haastattelun litterointiin, pitää varata aikaa neljästä kuuteen tuntia.

Haastattelujen litterointi on tutkimuksen analyysin kannalta erittäin tärkeä vaihe, koska litterointi on tapa ja mahdollisuus tutustua tarkemmin omaan aineistoon ja se on myös lähtökohta analyysin suunnittelulle. Litteroitaessa käsitys aineistosta muuttuu. Aineistoa kuunneltaessa ja kirjoitettaessa puhetta muistiin, näkyviin tulee asioita, joita tutkija ei välttämättä huomaa haastatteluvaiheessa. (Ruusuvuori & Nikander, 2017, s. 437)

3.4 Tutkimuksen luotettavuuden arviointi

Laadullisessa tutkimuksessa laadun ja luotettavuuden varmistaminen on tärkeää (Kananen, 2010, s. 68). Tutkimuksen tuloksiin pitää pystyä luottamaan, jolloin puhutaan tutkimuksen arvioitavuudesta (Koskinen ym., 2005, s. 253). Usein kuitenkin puhutaan reliabiliteetista ja validiteetista luotettavuuden arvioinnissa (Kananen, 2008, 123).

Aineiston sanotaan olevan reliaabeli, kun se ei sisällä ristiriitaisuuksia (Eskola & Suoranta, 2014, s. 214). Myös Koskinen ym. (2005, s. 255) toteavat reliabiliteetin liittyvän aineiston ristiriidattomuuteen. Kysymys on myös Hirsjärven ja Hurmeen (2009, s. 189) näkemyksen mukaan tutkijan tutkimusmateriaalista tekemän analyysin luotettavuudesta. Aineiston kattava käyttäminen ja tietojen litterointi ovat esimerkkejä tutkimuksen reliaabeliuksesta. Kuten myös, että tulokset heijastavat mahdollisimman pitkälle tutkittavien ajatusmaailmaa. (Hirsjärvi & Hurme, 2009, s. 189)

Validiteetilla ymmärretään, missä määrin tietty tulos, väite tai tulkinta ilmaisevat kohdetta, johon ne viittaavat, eli tutkitaan oikeita asioita. (Kananen, 2008, s. 123; Koskinen ym. 2005, s. 254) Yksinkertaisimmillaan Kanasen (2008, s. 123) näkemyksen mukaan validiteetti voidaan jakaa ulkoiseen ja sisäiseen validiteettiin. Sisäisellä validiteetilla (pätevyydellä) viitataan Eskolan ja Suorannan (2014, s. 214) mukaan tutkimuksen teoreettisten ja käsitteellisten määrittelyjen sopusointuun. Myös Koskinen ym. (2005, s.254) selittävät sisäisen validiteetin merkitsevän tulkinnan sisäistä loogisuutta ja ristiriidattomuutta. Voidaan puhua myös tulkinnan ja käsitteiden virheettömyydestä (Kananen 2008, s.123). Ulkoinen validiteetti voidaan ymmärtää tulosten yleistettävyytenä. Tämä tarkoittaa, että tulokset ovat siirrettävissä muihin vastaaviin tilanteisiin. (Kananen 2008, s. 123) Ulkoisen validiteetin nähdään olevan enemmän yhteydessä tutkijaan kuin tutkittavien käyttäytymiseen (Eskola ja Suoranta, 2014, s. 214).

Laadullisessa tutkimuksessa siis korostuu tutkimusprosessin luotettavuustekijät. Luotettavuuden arviointi kohdistuu koko tutkimusprosessiin, koska luotettavuuden mittarina toimii tutkimuksen tekijä. (Eskola ja Suoranta, 2014, s. 211) Laadullisessa tutkimuksessa luotettavuusarvion tekeminen on haastavaa (Kananen 2010, s. 68). Siinä korostuvat Kanasen (2008, s. 125) näkemyksen mukaan luotettavuuden pätevyyskriteerit, joita ovat vahvistettavuus, siirrettävyys, riippuvuus ja luotettavuus. Tutkimuksen laadun arviointi edellyttää laatukriteereiden rakentamista ja laadunvarmistusta tulee tehdä erilaisilla keinoilla opinnäytetyöprosessin kautta, toteaa (Kananen, 2008, s. 127). Myös Hirsjärvi ym. (2016, s. 232) nostavat esiin tutkimustyön kaikkiin vaiheisiin liittyvän tarkkuuden. Olosuhteet, jossa aineisto on tuotettu, on kuvattava selkeästi ja totuudenmukaisesti. Tarkkuutta lisää muun muassa aineistojen keräämisen kuvaaminen, millaisissa olosuhteissa haastattelut suoritettiin, havaittiinko häiriötekijöitä tai ovatko virhetulkinnat mahdollisia haastattelujen tai muun kerätyn materiaalin osalta. (Hirsjärvi ym., 2016, s. 232)

Tämän tutkimuksen näkökulmasta luotettavuus näkökohtiin kiinnitettiin erityistä huomiota koko prosessin ajan. Tutkija on kuvannut tarkasti olosuhteet, jotka olivat ominaisia tämän tutkimuksen tekemiselle. Kanasen (2010, s. 69) näkemyksen mukaan tutkimuksen uskottavuutta lisää, kun kaikki tutkimuksen eteneminen on dokumentoitu ja ratkaisut ja valinnat perustellaan työn eri vaiheissa tarkasti. Tässä työssä auttaa opinnäytetyöhön liittyvän päiväkirjan pitäminen, johon kirjataan kaikki toiminta, joka on vaikuttanut työn rakentumiseen (Kananen, 2010, s. 69).

Haastattelukysymyksiä rakennettiin koko teoriaosuuden rakentumisen ajan ja niitä peilattiin tutkimuskysymyksiin. Näin varmistettiin laatukriteereiden säilyminen koko tutkimuksen osalta yhdensuuntaisina. Myös haastattelujen toteuttaminen puolistrukturoituna, tukee keskustelevaa otetta haastatteluissa ja haastateltavalle annettiin mahdollisuus vastauksen antamiseen haluamallaan tasolla.

Haastateltavien luotettavuutta lisää myös se, että he kaikki ovat oman alansa huippuasiantuntijoita, osa jopa kansainvälisesti toimivia. Lisäksi tutkittava ilmiö liittyi kiinteästi haastateltuihin asiantuntijoihin. Tutkimuksen luotettavuutta lisää myös se, että akkrekoitujen virallisten auditoijien lisäksi suoritettiin kaksi haastattelua niin sanotuille

asiakasyritysten asiantuntijoille. Näillä haastatteluilla haluttiin tuoda esiin myös asiakkaan näkemyksiä auditointitilanteesta.

Tutkimuksen tekijä on pyrkinyt kuvaamaan mahdollisimman tarkasti tutkimusprosessin aikaisen toimintansa, jota on helppo seurata. Tähän lopputulokseen ovat tulleet myös Hirsjärvi ym. (2016, s. 232), jotka toteavat luotettavuuden ja pätevyyden arvioinnin tutkimuksen aikana tärkeäksi. Heidän näkemyksensä mukaan tutkijan tarkka selostus tutkimuksen toteuttamisen osalta nostaa laadullisen tutkimuksen luotettavuutta (Hirsjärvi ym., 2016, s. 232).

3.5 Aineiston analysointi

Tutkimuksen tekijä käytti paljon aikaa valmiiden litteroitujen haastattelukoosteiden läpikäymiseen. Materiaalista nousi esiin uusia näkökulmia ja ajatuksia, joita kirjattiin ylös päiväkirjaan tukemaan johtopäätösten tekemistä. Samanaikaisesti tutkimuksen tekijä teki myös merkintöjä haastatteluaineistoon tärkeinä pitämistään näkökulmista ja suunnitteli samalla materiaalin jatkokäsittelyä.

Haastattelut tuottivat riittävästi tutkimusmateriaalia. Litteroitu raakamateriaali sijaitsi tässä vaiheessa haastattelukohtaisilla word-dokumenteilla. Tutkija päätti siirtää niin sanotun raakamateriaalin excel-taulukkoon, mikä mahdollisti tutkimuksen vertailun. Tutkija alleviivasi raakamateriaali haastatteludokumentteihin tutkimuksen näkökulmasta tärkeimmät ydinaineistot, jotka siirrettiin excel-taulukkoon. Tutkimukselle tärkeät näkökohdat siirrettiin haastattelu ja kysymys kerrallaan matriisiin.

Tutkimusmateriaalin läpikäymisen yhteydessä tutkija tunnisti myös kokonaisuuteen liittyvät suorat haastattelulainaukset, jotka sijoitettiin samaan matriisiin edellä mainittujen ydinaineistojen kanssa sekä kiinnitettiin oikeaan asiayhteyteen. Suorat haastattelulainaukset esitetään sisennettynä lainausmerkkien sisällä. Lainauksissa mahdollisesti esiintyvät kolme pistettä (…) tarkoittavat tässä tutkimuksessa, että virkkeistä on poistettu sanoja, jotka eivät kuulu tämän tutkimuksen piiriin tai lainauksella olisi vaikutusta vastaajan tai kolmannen osapuolen anonymiteettiin. (Hirsjärvi ym., 2016, s. 120)

Jokainen matriisiin siirretty tekstiote sekä suora lainaus nimettiin tarkasti yksilöivällä tunnisteella. Akkretoidut auditoijat nimettiin juoksevalla kirjain-numeroyhdisteellä A1-A4. Samoin yritysasiantijoille annettiin tunnisteet Y1 ja Y2.

Kun raakamateriaali ja suorat lainaukset oli kiinnitetty matriisiin, tutkija käytti apunaan soveltuvin osin Gioia-metodia, joka mahdollistaa materiaalin työstämisen haastattelujen yksityiskohdista laajempiin teemoihin. Analysointia jatkettiin edellä mainitun raakamateriaalin ja lainausten koostamisen jälkeen laajempiin teemoihin ja lopulta etsittiin teemoille yhdistävät kokonaisuudet, ikään kuin yhdistäväksi sateenvarjoksi. Näitä teemoja on käytetty hyödyksi luvussa viisi. Edellä kuvattu haastattelujen analysointiprosessi ja eteneminen tulosten pohdintaan lisäsi tutkijan ymmärrystä aiheesta ja valmisti tulosten pohdintaan ja johtopäätösten kirjoittamiseen.

Seuraavaksi siirrytään tarkastelemaan haastattelujen tutkimustuloksia.

4 Tutkimustulokset

Tässä luvussa esitellään tämän tutkimuksen empiirisen osan tärkeimmät tulokset. Haastateltaville esitetyt kysymykset jakaantuivat neljään isompaan kokonaisuuteen, joita olivat lainsäädäntötarpeet, IoT-alustojen turvallisuusnäkökohtien ajantasaisuus, riskienhallinnan ja tietoturvan huomioiminen sekä viimeisenä auditointi. Haastattelutulosten esittely mahdollistaa tämän tutkimuksen lukijalle näkemyksen IoT-järjestelmien heterogeenisesta ympäristöstä ja havainnoista, joita haastateltavat nostavat esiin tutkimuksessa. Haastattelutulosten esittely avaa myös haastateltavien näkemyksiä siitä, pystytäänkö ISO 27001-standardin tietoturvallisuuden hallintajärjestelmällä arvioimaan jatkuvasti muuttuvia heterogeenisia IoT-ekosysteemeitä. Kaikilla haastatteluihin osallistuvilla eri organisaatioiden henkilöillä oli laaja kokemus ISO 27001 -auditoinneista. Haastatteluihin osallistuvien yrityksien henkilöillä oli kattava kokemus ja monipuolinen kosketuspinta myös IoT-alustojen ympäristöön.

4.1 Lainsäädäntötarpeet

Akkretoidut auditoijat

Virallisten akkretoitujen auditointiyritysten auditoijat arvioivat EU:n kyberturvallisuusasetuksen vaikutuksen olevan vähäistä nykyiseen toimintaan, eikä tilanteen oleteta muuttavan tilannetta lähitulevaisuudessa. Auditoijien näkemyksen mukaan EU:n kyberturvallisuusasetuksen vaikutukset alkavat näkymään toiminnassa, kun IoT-ympäristöön saadaan oma kriteeristö. Haastateltavat näkivät tämän kuitenkin kaiken kaikkiaan hyvin laajana kysymyksenä, johon ei ole yksiselitteistä vastausta. He totesivat myös, että tässä vaiheessa ei ole täysin selkeää, miten ja mihin eri osa-alueisiin EU-kyberturvallisuusasetus tulee vaikuttamaan. Todettiin myös, että lakiin liittyvät vaatimukset tulee nykytilanteessakin tunnistaa ja huomioida auditointeja tehtäessä. Lakivaatimusten todettiin olevan siis yksi auditointien osa-alue.

> ”Lakivaatimukset on yksi sidosryhmä, joka pitää tunnistaa ja hallita.” A4

Auditoijat arvioivat vapaaehtoisen tietoturvallisuuden hallintajärjestelmän arvioinnin olevan tehokas ja tietoturvan arviointimenetelmä. Vapaaehtoisuus nähdään tärkeänä elementtinä tarkasteltaessa myös tulevaisuuden arviointimenetelmiä. Tiedon arvon kasvaminen lisää suojaamisen tarvetta, tällöin haastateltavien näkemyksen mukaan, myös lainsäädäntöön liittyvien suojaamismäärittelyjen tarve kasvaa.

> ”Kun suojattavuus tulee tarpeeksi arvokkaaksi, niin kyllä valitettavasti lainsäädäntö on viimekädessä oleva keino.” A1

Auditoijat näkevät hyvin yksimielisesti tarpeen pakottavalle tietoturva-asetukselle, jotta tietoturvan tasoa saadaan kokonaisuutena nostettua. He nostavat esiin myös vaatimuksen uusien mahdollisten asetusten geneerisyydestä.

> ”Olisi joku vaatimus, että näin pitää tehdä, sen parempi.” A2

> ”Tällaiset lait ja asetukset edellyttää aina toimenpiteitä, siinä mielessä ne ovat hyviä.” A3

Kansallisen ja kansainvälisen tietoturvakriteeristöjen eroavaisuus nähdään haastateltavien auditoijien mielestä ongelmallisena. Kansalliset mallit tulisikin rakentaa paremmin linjassa kansainvälisten kanssa, haastateltavat toteavat. Ongelmallisina pidetään erityisesti kansallisia säädöksiä, Katakria, Vahtia ja Pitukria, jotka eivät ole yhteismitallisia IoT-tietoturva-arviointeja tehtäessä. Haastatteluissa hallintajärjestelmän auditoijat toivat selkeästi esille, että esimerkiksi muut kansalliset viranomaisauditoijat eivät välttämättä tunnista muita auditointimalleja tai muita ISO-sertifikaatteja, jotka ovat yleisesti käytössä kansallisissa auditoinneissa.

> ”Kansainvälinen lähestymistapa ja kansallinen lähestymistapa on auditoijan näkökulmasta ongelma, jos siellä on kaksi kriteeristöä ja erilaista filosofiaa.” A1

> ”Viesti asiakkaalta on se, että viime viikolla kävi Katakri arvioija ja nyt tulitte tai toisinpäin se on paremmin mennyt.” A2

Hallintajärjestelmän auditoijien mukaan, kansallisissa tietoturvakriteeristöissä (Katakri, Vahti, Pitukri), ei ole kaikkia niitä ominaisuuksia, jotka sisältyvät ISO 27001-standardiin. Hyvänä esimerkkinä haastateltavat nostavat esiin. riskienhallinnan ja sen jatkuvan parantamisen. Riskipohjaisuus on ISO 27001-standardissa isossa roolissa, kun taas kansallisissa tietoturvakriteeristöissä riskipohjaisuus haastateltavien näkemyksen mukaan käsitelty kevyesti.

> ”On siellä jotain pientä, kun mennään vähän syvemmälle, ISO:ssa on se jatkuva parantaminen ja riskilähtöisyys.” A1

Haastateltavat huomauttavat, että kansalliset tietoturvakriteeristöt ovat suunnattu ainoastaan kotimarkkinoille, eikä niitä ei tunnisteta missään muodossa ulkomailla. Auditoijat näkevätkin ongelmana, että kansallisesti yritetään säädellä sellaista toimintaympäristöä, joka on kansainvälinen ja tarvitsee kansainvälisen hallintajärjestelmän. Yksi auditoijista tuo esiin esimerkiksi Pitukrin ja toinen auditoija viittaa Katakriin, jotka molemmat ovat kansallisia tietoturvakriteeristöjä ja soveltuvat erilaisiin toimintaympäristöihin.

> ”Pitukri on siinä mielessä paljon ongelmallisempi, jo senkin takia, kun pilvipalvelut lähtökohtaisesti on kansainvälisiä ja idea on pilvessä.” A1

> ”Katakria ei tunneta Suomen rajojen ulkopuolella, sitten kysellään, että mistä sä puhut.” A2

> ”Että kyllä näissä samoja asioita, siis sama tavoitehan näillä kaikilla on ja ihan samoja käytäntöjä ja samoja vaatimuksia.” A2

Auditoijat näkevät kuitenkin kaikki kriteeristöt erittäin hyvinä turvallisuustoiminnan kehittämisen työkaluina yrityksille, olivat ne sitten kansallisia ja kansainvälisiä.

Yritysasiantuntijat

Yritysasiantuntijat näkevät EU:n kyberturvallisuusasetuksen vaikutuksen toimintaansa samalla tavalla kuin auditoijat. Toimintaan ei nähdä tulevan nopealla aikataululla muutoksia. Haastateltavien näkemyksen mukaan asetukselle olisi enemmän tilausta kuluttajapuolella. Kansainvälinen standardi ja siihen liittyvä turvallisuusleima antaisivat haastateltavien mukaan kuluttajille varmuuden siitä, että heidän hankkimansa laite on turvallinen.

Yritysasiantuntijoiden mukaan tämän hetken muutosvauhti on erittäin nopea IoT-puolella, kuvaava tilannetta sanalla ”hurja”. Haastateltavat nostivat esiin kysymyksen, mitä kaikkea IoT-laitteisiin liitetään ja ollaanko ympäristön muuttumisesta tarpeeksi tietoisia. Pakottavalle tietoturva-asetukselle nähtiin myös tässä ryhmässä tarvetta. Asetuksen avulla olisi mahdollista sisällyttää niin sanotut minimi tietoturvavaatimusten mukaiset asiat laitteen tai järjestelmän hallintaan. Yritysasiantuntijat herättivät kysymyksen toimenpiteiden kokonaisvaltaisuudesta, tehdäänkö oikeasti kaikki, mitä hallintajärjestelmän puitteissa pystytään tekemään ja takaako se lopulta tietoturvan osalta mitään.

> ”Se mistä aita on kaatunut, niin se saatiin juuri aikaiseksi.” Y1

> ”Aina löytyy niitä, jotka menevät alta riman.” Y2

Haastateltavissa herättää myös huolta IoT:n pilvipalveluympäristö ja syksyllä 2020 tapahtuneet tietoturvamurrot. Yritysasiantuntijat herättävätkin kysymyksen oikeasta tavasta toimia IoT-ympäristössä ja miettivät olisiko kuitenkin parempi luottaa enemmän standarditoimintaan kuin pakottaviin asetuksiin.

> ”Luotan kuitenkin enemmän, että on tätä standarditoimintaa, siihen sitä pohjuunnetaan kun ehkä asetuksiin.” Y1

Yritysasiantuntijat näkevät samoja päällekkäisyyksiä kansallisissa ja kansainvälisissä tietoturvakriteeristöissä, kuin auditoijatkin. Asiantuntijat viittaavat ongelmaan, jossa yhteistyökumppani saattaa vaatia toimintaa Pitukrin mukaisesti, toinen ISO 27001-standardin mukaan ja viranomainen sitten ehkä Katakrin mukaan.

> ”Ne katsoo vähän eri näkökulmasta asioita.” Y2

> ”Kaikkia on tullut vastaan ja niissä on päällekkäisyyksiä aika paljon.” Y2

Toinen asiantuntijoista nostaa esiin kansainvälisen liiketoiminnan vaatimukset ja tarpeet kansainvälisille sertifikaateille. Näissä tapauksissa kansalliset sertifikaatit eivät hänen mukaansa riitä.

4.2 IoT-alustojen turvallisuusnäkökohtien ajantasaisuus

Akkretoidut auditoijat

Auditoijat näkevät ISO 27001-liitteen A (27002), hyvin yleisenä kriteeristönä ja sen nähdään soveltuvan hyvin erikokoisten yritysten ja organisaatioiden käyttöön. IoT-alustojen turvallisuusnäkökohtien arviointi nähtiin yleisesti selkeänä. ISO 27001-standardi nähdään joustavana, koska se perustuu riskien arviointiin ja vaatimusten sekä riskien tunnistamiseen. Yrityksien ja organisaatioiden tulee kuitenkin ymmärtää toimintaansa liittyvät turvallisuusnäkökohdat. Organisaation tulee tunnistaa mitä tietoja sillä on käytettävissään ja miten suojattavat kohteet tunnistetaan, asiantuntijat toteavat.

> ”Soveltaminen pitää niin kuin ymmärtää, että mitä se soveltaminen sitten tarkoittaa.” A2

> ”Kyllä minun ensimmäinen kysymys on, että miten tämän applikaation tai systeemin tietoturvariskit on arvioitu.” A4

Turvallisuusnäkökohdat nostetaan esille riskiarviointien avulla auditoinneissa ja osoitetaan turvallisuuskontrollit, jotka liittyvät internettiin liitettyyn järjestelmään tai laitteeseen. Auditoijat kertovatkin näkevänsä ISO 27001-standardin niin sanottuna kontrollisettinä.

> ”Hyvä tietoturva rakentuu mielestäni siihen, että on hyvät menettelyt niiden riskien tunnistamiseen, vaarojen tunnistamiseen.” A4

Yksi haastateltavista nostaa esiin riskien tunnistettavuuden auditointitilanteessa. Jos auditoija ei tunnista IoT-ympäristössä olevia ongelmia, yritykselle voi jää mielikuva, että riskejä ei ole ja organisaation tietoturva toimii moitteettomasti.

Auditoijat viittaavat haastatteluissa IoT-alustojen tietoturvapuutteisiin, mikä tekee auditointitilanteesta hankalan. Tämä johtuu IoT-laitteiden heterogeenisestä toimintaympäristöstä ja soveltuvan standardin puutteesta.

> ”Mielestäni ollaan ihan asian ytimessä.”A2

> ”Tämän pitäisi vakioitua, että se pitäisi saada aikaan kansainvälisillä foorumeilla tällainen vaatimuskokoelma, joka sitten laajasti hyväksytään.” A2

Auditoijat joutuvat muun muassa aina miettimään käytetyn standardin käytettävyyttä arvioitavaan kohteeseen. Usein kuitenkaan yhden standardin käyttäminen auditointitilanteessa ei ole haastateltavan näkökulmasta riittävän monipuolista vaan rinnalle tarvitaan toinen avustava sertifikaatti. Auditoijien arviointitoimintaa vaikeuttaa erittäin laaja IoT- ekosysteemin käsite. He joutuvatkin tekemään usein arviointia yleisen standardin sopivuudesta kyseiseen kohteeseen. ISO 27001-standardi sopii auditoijien mielestä kaikille organisaatioille tietoturvallisuuden hallintajärjestelmänä.

> ”Laitteiden kirjosta johtuen tulee eteen se, että sopiiko juuri tällainen yleinen standardi, joka sopii vähän kaikille niin tähän ollenkaan.” A1

Auditoijat joutuvat siis jatkuvasti hakemaan mahdollisimman hyvin tilanteeseen sopivaa lisästandardia. Jos arvioitavaan kohteeseen ei löydy sopivaa arviointityökalua, auditoijat kertovat käyttävänsä yleistä ISO 27001-standardia. Auditoijat myös huomauttavat, että ISO

27001-standardin A-liitteestä löytyy kriteeristö ohjelmistojen kehitystyön arviointiin. Ongelmia aiheutuu haastateltavien mukaan myös usein siitä, jos auditoitava taho on valinnut jonkun tietyn standardin, joka ei sovellu kyseisen kohtaan arviointiin. Tällaisessa tapauksessa ongelmia voi esimerkiksi aiheuttaa auditoijan mukaan hyvin runsas laitteiden erilaisuus arvioitavassa kohteessa.

Auditoijien mielestä ISO 27001-standardi on kestänyt suhteellisen hyvin aikaa sen joustavuuden ansioista. Standardin nähdään olevan tällä hetkellä ajantasaisin tietoturvallisuuden hallintajärjestelmä. ISO 27001-standardi nähdään myös niin sanottuina yleisenä tietoturvastandardina, joka ei ole auditoijien mukaan erikoistunut mihinkään tiettyyn toimialaan, laitteisiin tai järjestelmiin.

> ”Minusta ISO 27001 on aika ajantasainen kuitenkin, kunhan organisaatio osaa itse soveltaa sitä omaan toimintaansa.” A4

Auditoijien haastatteluissa nousee esiin myös ISO 27001-standardin päivitystarpeet, joissa tulisi kiinnittää erityisesti huomiota IoT-ympäristöjen vaatimuksiin sekä käyttäjien yksityisyyden suojaan (privacy) tietojen käsittelyssä. Edellä mainitut kaksi esimerkkiä nousevat erityisen vahvasti esillä päivitystarpeina. Varsinkin ISO 27001-standardin liite A:n päivitystarve nostetaan haastatteluissa erityisesti esille. Yksi auditoijista nostaa esiin myös IoT:n ja sähköpostin välityksellä leviävät haittaohjelmat, jotka tulisi ottaa paremmin huomioon uudenlaisina uhkina. Tämä edellyttää haastateltavan näkemyksen mukaan tarkemmalle tasolle meneviä standardin vaatimuksia. Kasvavat riskit tulisi ottaa paremmin tarkasteluun auditoinneissa.

Auditoijat kertovat, että ISO 27001-standardia päivitetään parhaillaan. Yleisenä näkemyksenä voidaan todeta, että jos IoT-alusta on osa auditoitavaa hallintajärjestelmää, ISO 27001-standardissa on riittävästi yleisiä riskienhallintakeinoja käytettävissä.

> ”Siinä on peruselementit olemassa, mutta sitä ajantasaisuutta siinä tietysti tuoda lisää.” A2

Yksi auditoijista huomauttaa, että ISO 27001-standardista ei ole löydettävissä suoraan IoT-ympäristön ohjeita ja vaatimuksia. Myöskään tekninen tarkastus ei kuulu ISO 27001-standardin ominaisuuksiin.

> ”Teknistä tarkastustahan ei ISO 27001 piirissä ole, se on vain hallintajärjestelmä.” A3

Auditoijat muistuttavat, että ISO 27001-standardi ei itsessään sisällä valmiita vastauksia vaan organisaation on pyrittävä itse vastaamaan standardin tietoturvavaatimuksiin. Yritysten hallintajärjestelmät koostuvat haastateltavien mukaan erilaisista komponenteista ja organisaatioiden hallintamalleista, joten valmiita vastauksia toimintamalleiksi ei ole saatavissa. Organisaation on itse ymmärrettävä suojata kohteet vaatimusten mukaisesti ja toteutettava niille riskienhallintakeinot. ISO 27001- standardi vaatii yleisiä keinoja suojata kohdetta. auditoijat peilaavat aina vaatimuksia organisaation tekemisiin.

Yritysasiantuntijat

Toinen yritysasiantuntijoista pitää IoT:n turvallisuusnäkökohtia heikosti tunnistettavina ja usein epäselvinä. Tämä johtuu haastateltavan mukaan siitä, että IoT-laitteet kytkeytyvät aina suoraan johonkin pilvipalveluun tai keruulaitteeseen, jonka hallinnointimenettelyjä ei tunneta.

Myös toinen yritysasiantuntija nostaa esiin esimerkin omasta kokemuksesta, jossa kaksi eri kaupallista toimittajaa tarjosi IoT- alustapalveluja tilaaja organisaatiolle. Toinen toimittajista oli ISO 27001-sertifioitu ja toinen toimittaja oli ilman sertifiointia. Esimerkki tilaaja organisaatio eteni hankinnassa turvallisuus (security) edellä.

> ”Mennään security edellä, security tekee niitä vaatimuksia.” Y1

Edellä mainituista tarjoajista paljastui huomattavia eroja turvallisuuden suhteen. Haastateltava kertoo, että sertifioimattomassa yrityksessä kaikki kilpailutuksen osa-alueet oli otettu erityisen hyvin huomioon. Mutta ISO 27001-sertifioidulta yritykseltä organisaatio joutui pyytämään tarkennuksia hankintaprosessin aikana, lisäksi jouduttiin käymään keskustelua tilaajan toimeksiannon ymmärtämisestä. Tämä ISO 27001-sertifioitu yritys oli

tehnyt tarjouksen ISO 27001-vaatimusten perusteella. Prosessi oli haastateltavan mielestä kuvattu hyvin, mutta turvallisuusnäkökohdat (security) oli jätetty huomioimatta.

> ”Mulle jäi sellainen kuva, että ei se kerro mitään siitä, ovatko ne laitteet ja ne back end-serverijärjestelmät yhtään turvallisia.” Y1

Sertifioimattomassa yrityksessä palvelukokonaisuus oli rakennettu turvallisuusnäkökohdat edellä, eikä ISO 27001-standardin pohjalta.

> ”Että niin kuin toinen oli paljon vakuuttavampi, vaikka ne eivät puhuneet mitään ISO 27001-standardista.” Y1

> ”Ne oli nörttejä, jotka olivat tehneet sen esityksen ja ne puhu suoraan siitä, miten hoidetaan tietolähteen turvallisuus, pysyy täällä turvassa ja lähtee täältä turvallisesti.” Y1

> ”Ne oli mennyt IoT-turvallisuuteen minun mielestäni, eikä siihen prosessiin.” Y1

ISO 27001-standardi antaa yritysasiantuntijan mielestä toimintamallin organisaatiolle. Esiin nostetaan kuitenkin myös tarve lisästandardin käyttämisestä, koska useamman standardin käyttämisellä varmistetaan toiminnan turvallisuus.

IoT-alustoissa on haastateltavien näkökulmasta tietoturvaan liittyviä puutteita paljon, kuten myös niihin liittyvissä tiedonkeruulaitteissa ja sensoreissa, joiden kautta läpitunkeutuminen muihin järjestelmiin on mahdollista. Ongelmana tiedonkeruulaitteiden sensoreissa on haastateltavien mukaan valmistuskustannukset. Sensorit on valmistettu niin halvalla kuin mahdollista, jolloin tietoturva on unohtunut vaatimuslistalta.

> ”Tietoturva on just niin vahva kuin mitä siihen itse rakennat päälle.” Y1

Yritysasiantuntijoiden mukaan myös asiakasvaatimukset vaikuttavat kokonaisuuteen. ISO 27001-standardin vaatimusten lisäksi on huomioitava myös asiakkaiden omat vaatimukset esimerkiksi komponenttien käytölle, jotka eivät välttämättä ole standardin kanssa

yhdenmukaisia. Omaa IoT-järjestelmää rakennettaessa haastateltavan mielestä tulee huomioida myös kolmannen osapuolen komponentit.

> ”Kenen kaikkien toimittajien järjestelmiä on kiinni.” Y1

IoT-järjestelmää rakennettaessa, ongelmaksi muodostuu asiakkaan sekä kolmannen osapuolen tietoturvavaatimusten tunnistaminen. Huomioon on haastateltavan mielestä otettava ISO 27001-standardi, mutta myös mahdolliset ulkopuolelta tulevat vaatimukset.

Yritysasiantuntijat pitävät pelkkää ISO 27001-standardia riittämättömänä IoT-alustojen auditoinnissa. He näkevät, että tarvitaan myös toinen arviointityökalu tai lisästandardi avuksi, jolloin kokonaisuus saadaan tarkemmin arvioitua ja tietoturvallisemmaksi. IoT-toimintaympäristö on erittäin vaativa auditoinnin näkökulmasta ja vaatiikin haastateltavien mukaan auditoijalta erityistä ammattitaitoa soveltaa ISO 27001-standardia kyseisessä ympäristössä.

> ”Mutta auditoijan merkitys korostuu siinä kohtaa.” Y2

> ”Miten joku asia on toteutettu, vaan enemminkin, että ne asiat pitää olla huomioitu ja dokumentoitu.” Y2

4.3 Riskienhallinnan ja tietoturvan huomioiminen

Akkretoidut auditoijat

Auditoijat näkevät uudenlaisten tietoturvariskien havainnoinnin IoT-järjestelmäympäristössä haastavana. Esiin nousee erilaisia hallittavuusominaisuuksia ja havainnointikyvyn sekä muutoksenhallinnan puutteita, jotka johtavat uudenlaisiin tietoturvariskeihin, joita ei tunnisteta.

> ”Jos edelliset vastaukset olen yrittänyt pitää konkreettisena, niin tämä menee ohueen yläpilveen.” A1

> ”Pelkästään sen vuoksi, että en tiedä kaikkia riskejä.” A1

Auditoijat nostavat esiin, miten laiteympäristöä, alustaa ja verkkoa voidaan käyttää hyväksi negatiivisessa ja positiivisessa mielessä. Laiteympäristöt muodostavat hallittavan kokonaisuuden, jota ohjataan jostain tietystä sijainnista. Tämä vaatii jatkuvaa osaamisen ja tietoisuuden sekä toiminnan läpinäkyvyyden kehittämistä. Ylläpitäjälle pitäisi olla auditoijan mukaan selkeää, mitä tietoja laitteissa ja ohjelmistoissa on ja mistä alustaan tai ympäristöön tuodaan tietoja. IoT:n heterogeeninen ympäristö johtuu eri valmistajien laitteiden erilaisista kyvykkyyksistä sekä erilaisella kypsyystasolla olevista turvajärjestelmistä ja kontrolleista, jotka haastateltavien mukaan pitäisi huomioida muutoksenhallinnassa. Haastatteluissa nousi hyvin vahvasti esiin muutoksenhallinnan prosessin tärkeys. Muutoksenhallintaa tulisi auditoijien mukaan tehdä pienistäkin, jopa turhalta tuntuvista muutoksista ja sellaisista muutoksista, jotka eivät suoranaisesti johdu jonkun laitteen tai ohjelmiston muutoksesta tai lisäyksestä hallittavaan järjestelmään.

> ”Menee tietyllä tavalla sen riskienhallinta laatikon ulkopuolelle siinä mielessä, että siinä tarttee olla toimintakyky, joka kykenee reagoimaan semmoisiin täysin outoihin tilanteisiin.” A1

Muutoksenhallintaan ei auditoijien mielestä ole kiinnitetty tarpeeksi huomiota IoT-järjestelmien hallinnassa, koska nopeasti muuttuva IoT- ympäristö tuo siihen erityisiä haasteita. Uhkia ja uusia teknologioita tulee entistä nopeammin. Perinteinen muutoksenhallinta on usein liian hidas ja se ei haastateltavien mielestä sovi IoT-ympäristöön. Muutoksenhallinnan pitäisi olla heidän näkemyksensä mukaan reaktiivista, koska mahdollinen nopeasti leviävä tietoturvaongelma mahdollistaa vakavan riskin toiminnassa. Tästä nousee esiin ketterä muutoksenhallinta, joka auttaa reagoimaan nopeammin muuttuviin asioihin.

> ”Jos on iso haavoittuvuus, niin varmasti reagointiaika tulee lyhyemmäksi, muutoksenhallinnassa pitäisi kyetä arvioimaan myös taaksepäin tapahtuvat vaikutukset sen ominaisuuksiin.” A1

> ”Kyllä ne standardin vaatimukset täyttää, mutta ovatko ne tehokkaita ja hyviä, se on vähän eri asia.” A4

Muutoksenhallinta tulisi nähdä koko organisaatiossa tapahtuvien muutosten analysointina, joka tulisi ulottaa ylimmästä johdosta, läpi organisaation sekä arvioida muutosten vaikutus liiketoimintaan. Auditoijat näkevät myös, että muutoksenhallinnassa tulee huomioida lisäksi sidosryhmissä tapahtuvat muutokset. Näitä muutoksia voivat olla erilaiset toimittajien tai palveluntuottajien toimintaympäristössä tapahtuvat muutokset. Tällainen muutos voi olla esimerkiksi palveluntuottajan muuttaminen uuteen toimipaikkaan.

> ”Varautuminen sellaiseen, johon ei osaa ennakolta varautua, niin se tulee tässä IoT- maailmassa entistä tärkeämmäksi.” A1

> ”Mä väitän, että muutoksenhallinnassa on valtavia puutteita.” A2

> ”Jos jossain organisaatiossa insinööripohjainen toimitusjohtaja väistyy ja tilalle tulee finanssi numeronikkari toimitusjohtaja, niin puolen vuoden päästä voi lyödä veikkaa, se on ihan erilainen firma.” A4

Auditoijat näkevät ymmärtämättömyyden muutoksenhallinnan suurimpana puutteena. Auditoitava asiakas ei välttämättä ymmärrä, mikä on suojattava kokonaisuus, jota hallintajärjestelmässä suojellaan. Toinen vahvasti esiin nouseva asia auditoijien näkökulmasta on muutoksesta johtuvien riskien tunnistaminen ja niistä aiheutuvat ongelmat. Auditoitavan asiakkaan tulisi ymmärtää muutoksenhallinnan tärkeys, sekä mahdollisten muutosten aiheuttamat muutokset hallittavassa järjestelmässä.

> ”Yksi teollisuuden toimittaja, joka oli sitten yhtäkkiä keksinyt, että mehän liitetään nettiin nämä härpäkkeet, sitten kun me alettiin käymään läpi niitä turvallisuustoimintoja niin se oli niin kuin, että tukka nousi pystyyn, ei siellä mitään ollut.” A2

> ”Se lähtee siitä, että ymmärretään se tiedonhallinta.” A3

> ”Ei riitä tässä maailmassa vaan sun täytyy olla aika lailla aktiivinen koko ajan käytännössä.” A2

Auditoijat toteavat, että organisaation pitää havainnoida ja tunnistaa toimintaympäristössä tapahtuneita muutoksia ja reagoida niihin tarvittavilla keinoilla. Muutos voi olla ulkoinen tai sisäinen tekijä, joka organisaation tulee omassa toimintaympäristössään arvioida. Toimintamalleja tuleekin arvioida haastateltavien mukaan kriittisesti.

Myös yhteyksien tärkeys erilaisiin osaamisyhteisöihin nousevat esiin haastatteluista. Erilaiset osaamisyhteisöt tukevat organisaatiota oman tietoturvan kehittämisen apuna, tämä tieto voi auttaa tunnistamaan uusia riskejä omassa organisaatiossa sekä saada tietoturvaan liittyvää uhkatietoa. Osaamisyhteisöt myös jakavat tietoa ja niissä voi vaihtaa kokemuksia nopeasti muuttuvasta ympäristöstä. Auditoija toteaa, että näissä osaamisyhteisöissä on paljon niin sanottuja valkohattuhakkereita, joilta saatu tieto on erittäin arvokasta.

> ”Siellä tapahtuu niin nopeasti asioita, että mitä enemmän on mukana osaamisyhteisössä ja foorumeissa ja osallistuu sinne ja sieltähän löytyy myös mahdollisia riskejä näille omille laitteille ja järjestelmille.” A4

Riskienarviointia tehdään jatkuvasti yrityksien muuttuvissa IoT- järjestelmissä erilaisilla riskienhallinnan menetelmillä. Auditoija toteaa, että jokainen yritys tekee riskienhallinnasta oman näköisensä. Auditoijat näkevät suuria puutteita riskienarviointimenetelmissä ja muutoksenhallinnassa. Yrityksien riskienhallinnassa ei auditoijien näkemyksen mukaan osata tarpeeksi kiinnittää etukäteen huomioita hallintajärjestelmissä tapahtuviin asioiden muutoksiin. Tähän vaikuttavat myös heikot riskienarviointimenetelmät. He näkevätkin, että organisaatiossa ei ymmärretä, mitä suojattavaan ominaisuuteen kuuluu ja pienetkin muutokset voivat aiheuttaa ennalta arvaamattomia riskejä. Näillä riskeillä on suuri vaikutus yrityksen hallinnassa olevaan järjestelmään ja sillä on vaikutus myös yrityksen toimintaympäristöön.

> ”Sit vaan sattuu näitä juttuja ja tulee lantaa tuulettimeen.” A1

> ”Tyyppitilanne on, että muutoksenhallinnalla ja riskienarvioinnilla ei ole mitään kytkentää.” A2

> ”Minusta riskienarviointi on aika huonolla tasolla.” A4

Esiin nousee asioita, joihin yrityksien tulee auditoijien mukaan kiinnittää enemmän huomiota: resursseja pitää varata riittävästi asioiden hoitamiseen. Riskienhallinta pitäisi huomioida IoT-järjestelmissä jatkuvalla testaamisella sekä toiminnan ajantasaisuudella. Muutoksia tehdään hallintajärjestelmiä sisältävien laitteiden toimintaympäristöön, mutta muutoksesta aiheutuvia riskejä tietoturvaan tai tietojen suojaamiseen ei osata arvioida riittävän monipuolisesti. Muutokset pitäisi tunnistaa ja muutokseen liittyvät mahdolliset riskit. Lisäksi auditoijat toteavat, että on tärkeää myös arvioida riskin vaikutusta toimintaan monipuolisesti.

”Siinä pitää katsoa eheys, saatavuus, luottamuksellisuus ja käytettävyys.” A3

Osa auditoijista huomauttaa, että kaikkia asioita on mahdotonta todeta ja ottaa huomioon riskienhallinnassa, jossa nousee esiin myös nopeus riskien ennakoinnissa. Nopealla reagointikyvyllä pystytään ottamaan asia hoidettavaksi ja reagoimaan riskiin sen vaatimalla tavalla, jotta eskaloitunut tilanne saadaan siedettävälle tasolle.

Riskienarvioinnin pitäisi olla vahvasti ennakoivaa, jolloin asian käsittelyyn olisi riittävästi aikaa ennen muutoksen toimeenpanoa. Auditoijat huomauttavat, että riskienarviointimenetelmistä aiheutuu aina keskustelua ja varsinkin niiden tasosta; ovatko arviointimenetelmät riittävän hyviä arvioitavaan kohteeseen. Uusia riskien havainnointimenetelmien käyttöönottoa IoT-ympäristössä auditoijat pitävät vaikeana, johtuen järjestelmien heterogeenisesta ympäristöstä.

”Ongelma heikot riskienarviointimenetelmät.” A4

Osa auditoijista tuo esiin, että ISO 31000-riskienhallinta standardin käyttöönottoa kannattaa harkita omassa ympäristössä sisäisenä lisätyökaluna. Tämä standardi onkin haastateltavien mukaan aika yleisessä käytössä yrityksissä. Muutos on riski, jota voidaan kontrolloida.

Yritysasiantuntijat

Yritysasiantuntijat näkevät uhkien lisääntyvän kiihtyvällä tahdilla, jolloin asiantuntemuksen pitää pysyä organisaatiossa todella korkealla tasolla.

> ”Niin tuota eihän siinä oikein mistään muusta, kuin että se asiantuntemus pitää olla huipussaan siinä yrityksessä, pitää olla projektinhallinta hyvä, sen prosessit hyvä ja nimenomaan riskien kartoitus pitää olla hyvällä tasolla.” Y1

Toinen yritysasiantuntija nostaa esiin saman näkemyksen kuin auditoijat. Organisaatiossa tulee kiinnittää huomiota yrityksen toimintaympäristöön ja muutoksenhallintaan, omistajuussuhteisiin, näillä on haastateltavan näkemyksensä mukaan vaikutusta muun muassa turvallisuusasioihin. Kehityksen vauhti nähdään erittäin kovana ja jo vuodessa tapahtuu erittäin isoja muutoksia sekä kehitystä erilaisissa IoT- laitteissa. Ympäristön muutoksia onkin haastateltavan näkemyksen mukaan tärkeää seurata. Toinen yritysasiantuntija nostaa esiin myös kysymyksen, osataanko oikeasti tunnistaa uudenlaisia tietoturvariskejä. Tunnistaminen vaatii osaamista ja uudenlaisia tietoturvariskejä tulee esiin kiihtyvällä tahdilla.

Yritysasiantuntijat nostavat esiin samoja asioita riskienhallinnasta kuin auditoijat. He näkevät riskienhallinnan muuttuvassa IoT-ympäristöissä erittäin tärkeänä, jota pitäisi tehdä säännöllisin väliajoin erittäin laaja-alaisesti. Toinen yritysasiantuntijoista toteaa, että kaikki auditointijärjestelmät ovat menneet entistä enemmän riskienhallintapohjaiseksi. Yritysasiantuntijat pitävät hyvänä riskienhallintamallina, jossa työntekijät tunnistavat toiminnasta riskejä ja ilmoittavat niistä havaintoja.

> ”Havainnot tarvitaan kentältä, en minäkään usko siihen, että se suunnitteluporukka kaikkia niitä riskejä keksi. Itse laitteen pitäisi pystyä ilmoittaan, kaikki hakkerointi yritykset esimerkiksi.” Y1

> ”Niin toki siinä on iso rooli henkilöstöllä, että he tuovat esiin niitä havaitsemiaan asioita.” Y2

Työntekijöiden tunnistamat riskit arvioidaan vaadittavien asiantuntijoiden kanssa organisaation riskienhallintajärjestelmässä. Yritysasiantuntijat näkevät tärkeänä, että maailmalta tunnistettua riskitietoa pystyttäisiin hyödyntämään oman organisaation käytössä. Järjestelmien tietoturva-aukoista ja mahdollisista tulisi saada palautetta nykyistä nopeammin. Toinen yritysasiantuntija tuo esiin tekoälyn hyödyntämisen tai yhteistyörobotin käyttämisen riskien analysoinnissa.

Myös yritysasiantuntijat tuovat esiin muutoksenhallinnan tärkeyden, joka on yksi tärkeimpiä asioita IoT- järjestelmiä hankittaessa. Muutoksenhallinta on vaikeaa, jos organisaatiolta puuttuu osaaminen. Kaikki muutokset, jotka järjestelmän kokoonpanoon tehdään, tulisi arvioida etukäteen huolella ennen käyttöönottoa.

4.4 Auditointikäytännöt

Akkretoidut auditoijat

Hallintajärjestelmän auditoinneissa IoT-laitteita sisältävien erilaisten rajapintojen vaikutusten tunnistaminen on haastateltavien näkemyksen mukaan mielenkiintoista.

Iot-laiteympäristössä on paljon erilaisia mielenkiintoisia rajapintoja, joiden vaikutukset tietoturvallisuuteen ja riskienhallintaan tulee haastateltavien näkemyksen mukaan tunnistaa auditointitilanteessa. Auditoijat kertovat laajuuden määrittelyn olevan auditoijan tärkein työkalu. Jos laitteet ovat hallintajärjestelmän kattavuusalueella, niin tällöin ne otetaan huomioon auditoinnissa. Haastateltavat kertovat, että auditoinneissa määritetään tarkat rajapinnat auditoitavalle kokonaisuudelle.

> ”Auditoijan yksi tärkein työkalu on se laajuuden määrittely, skouppaus.” A1

Auditoijat ovat myös huomanneet erilaisiin rajapintoihin pysähtyvän vastuun. Tällaisissa esimerkkitapauksissa toimittaja A lähettää dataa analysoitavaksi toimittaja B:n järjestelmään, jolloin auditointi ei enää ulotu B- järjestelmähallintaan. Yleisesti IoT-laitteet tuottavat pilvestä palvelua, josta kerätään tietomassaa niin sanottua big dataa, haastateltava kertoo. Tätä tietomassaa käytetään eri järjestelmien ohjauksiin sekä analysoidaan dataa ja rikastetaan tietomassaa. Hyvänä esimerkkinä eräs auditoija nostaa kiinteistöautomaation eli kiinteistön hallintajärjestelmän tuottaman IoT-datan, jolla ohjataan kiinteistön laitteistoa. IoT- järjestelmä ei ole kuitenkaan auditoinnin piirissä, koska se ei kuulu arvioitavaan kokonaisuuteen. Tästä syystä auditoijat pyrkivät käymään tarkkaan kaikki rajapinnat läpi, minkälaisia palveluita- ja järjestelmiä auditoitavalla organisaatiolla on sekä miten niitä hyödynnetään.

> ”Yritin vähän kyselläkin IoT- juttuja, mutta ne eivät ole nyt sitten heidän vastuullaan, heidän johtamisjärjestelmän ulkopuolella.” A1

Haastateltavat toteavatkin, että käyttöön pitäisi saada uusia elementtejä, joilla kyettäisiin analysoimaan rajapintoja paremmin, eli ymmärrys, mistä osasta asiakasyrityksen hallintajärjestelmää kyseinen yritys vastaa. Yrityksen tulisi huomioida sen omaan tietoturvaan liittyvät näkökohdat, kun se hallinnoi asiakkaan käytössä olevaa laitetta. Auditoijat nostavat esiin kysymyksen, mahdollistavatko puutteet auditointirajapinnoissa kanavan ulkopuolisille hyökkäyksille ja pääsyn arvokkaaseen dataan.

> ”Auditoijan pitäisi ajatella, miten olette tämän IoT-puolen tietoturvan hanskanneet, teillä on tosiaan vastuu siitä, että se työstökeskus ei ala porailemaan ihan omiaan.” A1

> ”Niin siinä on kuitenkin se, että kun ne vastaa paitsi (…) laitteen tekemisestä myös (…) laitteesta ja sen verkottuneesta maailmasta, niin auditointimielessä se skoupin rajaus pitäisi jollain tavalla ajatella, se pitäisi ottaa mukaan.” A1

Perinteisesti kaikki yrityksen toimipisteet ja liiketoiminnan osa-alueet ovat olleet osa auditointiprosessia. Haastateltavan mukaan, toinen vaihtoehto on rajata joitain liiketoiminnan osa-alueita auditoitavan hallintajärjestelmän ulkopuolelle. Auditoijat painottavat hallintajärjestelmän auditoinnissa eheyden, saatavuuden, luottamuksellisuuden sekä tiedon ja omaisuuden hallinnan osa-alueita. Auditoijat kertovat tarkastelevansa hallintajärjestelmään liittyviä pääomia, missä ne sijaitsevat ja minkä tyyppisiä pääomat ovat. Huomio kiinnittyy myös vastuisiin ja valtuutuksiin sekä edellä mainittujen käyttämiseen. Myös auditoitavien laitteiden sijaintiin ja yhteyksiin liittyvät asiat tulee selvittää auditoinnin aikana. Eräs auditoija nostaa esiin tarpeen IoT- lisähallintakeinoista, joka pitäisi sisältyä tai kuulua ISO 27000 sarjaan.

> ”Mielestäni pitäisi olla 27001 kanssa joku 27-sarjaan sisältyvä tai kuuluva dokumentti, jossa olisi lisähallintakeinot.” A2

Haastateltavat tunnistavat IoT-pohjaisen pilvipalvelun auditoinneissa useita tietoturvaongelmia. Näistä havaituista ongelmista auditoijat joutuvat kirjoittamaan

poikkeaman tai poikkeamia. He toteavat, että kaikki poikkeamat liittyvät tietoturvan kolmeen pääaiheeseen; eheyteen, saatavuuteen ja luottamuksellisuuteen. Auditoijat nostavat esiin myös jatkuvuudenhallinnan tärkeänä näkökulmana. IoT-ympäristössä laitetoimintaan liittyy suurena kysymyksenä myös pilvipalvelun käyttökatkokset. Haastateltava nostaa esiin organisaation varautumisen käyttökatkoksiin riskienhallinnan näkökulmasta. Organisaation tuleekin arvioida, minkä asteista riskiä se sietää käyttökatkoksien osalta ja millainen toimintamalli sillä on suunniteltu pilvipalvelujen käyttökatkoksien ajaksi. Miten toimitaan, kun kyseinen palvelu ei ole enää käytössä, haastateltava toteaa.

> ”Mutta kun siinä on paljon muitakin komponentteja välissä, että on tietoliikennettä ja mennään muiden valtioiden alueiden läpi, valokuidulla tai millä mennäänkin niin siinä on kaiken maailman potentiaalisia häiriötekijöitä, jotka vaikuttavat siihen saatavuuteen ja jatkuvuuteen voi vaikuttaa vakavasti.” A2

> ”Auditoinnissa sitten kysytään onko näitä asioita riskilistalla tai toisin päin mitä olette näille tehneet. Tulee vähän tyhjiä katseita, että älä nyt viitsi, kyllä Azure on aina pystyssä.” A2

> ”Aika monella on käsitys, että Azure tai AVS ei ole ikinä alhaalla.” A2

> ”Näitä ei mielestäni ole tarpeeksi otettu huomioon.” A2

Toisena huomionarvoisena asiana auditoijat tuovat esiin pääsynhallinnan, jolla määritetään pääsyoikeudet käyttäjätasolla järjestelmiin sekä peruste käyttöoikeudelle. Toimittajien ja kolmansien osapuolten palveluntuottajien hallintaan liittyvät asiat tulee arvioida aina riskiperusteisesti. Pääsyoikeuksien hallinnassa nousee esiin myös kolmansien osapuolien pääsyoikeuksien jako, jonka auditoijat näkevät ongelmallisena. Pääsynoikeuksien hallintaa tulisikin haastateltavan mukaan arvioida omassa organisaatiossa säännöllisin välein ja kiinnittää erityisesti huomiota siihen, ovatko oikeudet tarvittavilla henkilöillä ja ovatko oikeudet ajantasalla. Kolmantena haastatteluista esiin nousseena asian oli riskienhallinnan tunnistaminen ja arviointi. Riskien tunnistamiseen ei auditoijien näkemyksen mukaan ole asiakasyritykset perehtyneet, jolloin kaikkia tietoturva-aukkoja ei välttämättä tunnisteta.

> ”Useasti riskienhallintatyökalut näyttää ihan hienolta, mutta kun mennään ns. lattialle tai tuotantoon katsomaan asiaa mitä siellä tehdään oikeasti. Sitten huomataan miten täällä olevat asiat liittyvät riskienhallintaan.” A4

Tietoturva-aukkojen muodostuminen liittyy auditoijien näkemyksen mukaan suuresti hallittavan järjestelmän käyttötapaan, IoT-järjestelmän muodostamaan kokoonpanoon sekä maantieteelliseen sijaintiin. Auditoijat nostavat esiin myös ennakoinnin puutteen, josta ISO 27001-standardissa on vaatimuksia.

Auditoijat ovat huomanneet, että ISO 27001-standardin auditoinneissa nousee vahvasti esiin hallintajärjestelmän osaamisen ja resurssien puute. Heidän mukaansa erityisesti osaamiseen tulee kiinnittää huomiota käytettäessä hallintajärjestelmää. Kokonaisuuksien ymmärtäminen on tärkeää, organisaation tulee ymmärtää eri osa-alueet, joista standardin vaatimukset muodostuvat. Auditoijat painottavat myös, että organisaation johdolla on vastuu tunnistaa hallintajärjestelmässä tarvittava osaaminen ja osoittaa resurssit.

> ”Jos mä sanon, että 95 % vastasi eri sanamuodoilla, mutta taustalla piili aina osaaminen. Osaavat henkilöresurssit.” A2

> ”Vähän kuin, että viedään se auto katsastustoimistolle ja katsotaan mitä vikoja siinä on. Vikalista ja sitten se lista on niin pitkä, että ne mietti, että ei perkule, onkohan meillä resursseja ylipäätään ottaa tätä.” A4

> ”Että ollaan arvioivinaan riskejä, mutta sitten kun niitä on listattu johonkin, ei ole ymmärretty, ei viitsitä, uskalleta tai jakseta – mikä se syy onkaan. Väittäisin, että siinä tulee jossain kohdin se osaaminenkin vastaan ja viedä niitä asioita eteenpäin.” A1

Organisaatiosta tulee löytyä auditoijien mukaan tarvittavat resurssit niin tekniseen osaamiseen kuin johtamiseenkin. Tarvittavilla asiantuntijolla tulee olla haastateltavien mukaan tekninen osaaminen ja erityisesti johdolla tulee olla ymmärrys ja kokonaisymmärrys standardin vaatimuksista. Puhuttaessa tietoturvallisuudesta, IoT-ympäristöstä, digitaalisesta maailmasta sekä digitaalisesta turvallisuudesta, nousee osaamisen rooli auditoijien näkemyksen mukaan tärkeimmäksi kyvykkyydeksi.

> ”Semmoinen niin kuin tekninen osaaminen, että joku ymmärtää vähän, oli se organisaatio nyt sitten millainen hyvänsä. Tunnistaa vähän mitä me täällä tehdään ja mitä laitteita meillä on ja miten näitä pitäisi alkaa hallitsemaan.” A4

> ”Sitten kun mennään syvemmälle niin AVS:n palomuurien konfigurointia. Niin siellä tarvitaan jo vähän oikeesti osaamista. Näppäröintiosaamista.” A4

Hyvin usein haastateltavien mukaan ISO 27001-standardin hallintajärjestelmän kehittämisessä organisaation ylin johto ei ymmärtänyt mistä standardin käytössä on kysymys ja mitä sen kehittäminen tarkoittaa organisaation toiminnalle. Tietoturvallisuuden hallintajärjestelmä vaatii organisaation eri toiminnoilta osaamista ja ymmärrystä lain tulkinnasta sekä mitä hallintajärjestelmä vaatii asiakkaiden ja sidosryhmien hallinnalta. Usein organisaatio keskittyy vain hallintakeinoihin huomioimatta lainkaan esimerkiksi riskienarvioinnin ja muutoksenhallinnan välistä yhteyttä, jotka pahimmassa tapauksessa voivat puuttua kokonaan, auditoija toteaa.

> ”Että jos ylin johto ei ymmärrä muuta kuin se, että asiakas on vaatinut, että teillä pitää olla joku ISO 27001.” A4

> ”Ylimmän johdon osaaminen ja näprääjät, jotka oikeasti tekee asioita ja ovat ajan tasalla. Nämä kaksi asiaa.” A4

Organisaation johdon tuleekin nähdä ja ymmärtää haastateltavan näkemyksen mukaan tarvittavien investointien tarve hallintajärjestelmään ylläpidossa. Hän jatkaa, että usein järjestelmään tehtävät tietoturvallisuuden kehittämistoimet nähdään kuluina, johon ei haluta investoida. Hallinnointijärjestelmän ylläpitäjillä tuleekin olla organisaation johdon täydellinen tuki järjestelmän kehitystyön osalta. Tarvittavat turvallisuuteen liittyvät investoinnit maksavat itsensä nopeasti takaisin, eikä mahdollista maineen menetystä tule huonon tietoturvallisuuden takia. Organisaation johdon on ymmärrettävä, että tietoturvallisuuden ylläpitäminen vähentää toiminnan riskejä ja suojelee osaltaan yrityksen brändiä.

Yritysasiantuntijat

Yritysasiantuntijoiden näkemyksen mukaan auditoijilla on suuri vastuu löytää IoT-hallintajärjestelmään sisältyvät tietoturvan mahdolliset poikkeamat auditoinneissa. Auditoijan osaamisessa korostuu taito osata tarkastaa ja kysyä hallintajärjestelmän auditoinneissa IoT-ympäristöön liittyvistä asioista. Haastateltavien mielestä auditoijan laaja-alainen osaaminen nostaa myös sertifioinnin arvostusta.

> ”Jää tosi paljon sen auditoijan osaamisen vastuulle. osaako tarkistaa sekä kysyä tuohon liittyvät asiat.” Y2

Auditoija tutustuu yrityksen auditoitaviin toimintoihin muutamien dokumenttien ja keskusteluiden kautta, minkä perusteella auditoijan pitäisi pystyä tarkistamaan hallintajärjestelmän kokonaisuuteen kuuluvat asiat sekä tekemään johtopäätökset tietoturvan tasosta. Haastateltavat näkevät tämän haastavana kokonaisuutena ja korostavan auditoijan osaamisen tasoa.

IoT-järjestelmien kokonaisvaltainen tietoturva-aukkojen tunnistaminen auditoinneissa herättää kysymyksiä yritysasiantuntijoissa. IoT-järjestelmän hallittu käyttö vaikuttaa keskeisenä asiana tietoturva-aukkojen syntymiseen, tällä on vaikutusta käyttöympäristöön.

Haastateltavat mainitsevat käyttöympäristöön liittyvien käyttötapausten paremman huomioimisen auditoinneissa. Pääsynhallinnan puutteet ja toteutus nousevat esiin myös yritysasiantuntijoiden näkemyksissä.

> ”Voi olla, että käytät järjestelmää, vaikka roskapönttöjen täyttöasteen mittaamiseen, milloin kannattaa tyhjentää astia tai autonomisen ajoneuvon ohjaamiseen, nämä on kaksi ihan eri asiaa.” Y1

Myös yritysasiantuntijat tuovat esiin osaamisen puutteen organisaatioissa IoT-käyttöympäristön osalta. Osaamiseen ja kouluttamiseen liittyy vaatimuksia ISO 27001-standardissa. Yrityksissä saattaa olla puutteita tai erilaisia toimintoja, joita ei haastateltavien mukaan ole yksinkertaisesti osattu ottaa huomioon, ja ne tulevat esiin vasta auditointia tehtäessä. Yritysasiantuntijat näkevät tärkeänä, että hallintajärjestelmän auditoija nostaa

esiin organisaation osaamiseen liittyvät ISO 27001-standardin ylläpitoon liittyvät osaamistarpeet.

5 Tulosten tarkastelu, pohdinta ja johtopäätökset

Tässä luvussa tarkastellaan haastattelujen tuloksia teoreettiseen viitekehykseen sekä aikaisempien tutkimuksien tuloksiin. Tutkija pohtii ja vertailee akkretoitujen auditoijien ja IoT-yritysasiantuntijoiden haastattelujen tuloksia alati muuttuviin heterogeenisiin IoT-alustoihin liittyviin standardin vaatimusten soveltuvuutta IoT-alustojen riskeihin ja niiden hallitaan. Lisäksi tarkastellaan ISO 27001-standardin soveltuvuutta IoT-laitteita sisältävien alustojen hallintajärjestelmien arviointiin.

Samalla esiin nostetaan mahdollisia tutkimusmateriaalista esiin nousevia samankaltaisuuksia tai eroavaisuuksia tarkasteltaessa saatuja tuloksia sekä teoriaa. Tämän jälkeen tarkastellaan tutkimuksen johtopäätöksiä sekä vastataan tutkimuskysymyksiin.

5.1 Lainsäädännön ja ohjeistuksen näkökulma

Tutkimuksessa akkretoitujen auditoijien sekä yritysasiantuntijoiden haastatteluissa nousi esiin monia lainsäädäntöön ja ohjeistukseen liittyvää huomioita, jotka liittyivät IoT-laitteita sisältäviin palvelualustoihin ja joiden riskienarviointia on tehty ISO 27001- standardin perusteella. ISO 27001- standardi on kansainvälinen standardi, jonka muutokset ja uudistaminen hyväksytetään aina järjestöön kuuluvilla jäsenvaltioilla. (SFS-EN ISO/IEC 27001/2017, s. 4) Haastateltava toteaa, että standardi on uusiutunut noin 3–4 vuoden välein ja **hyväksyttämisprosessi koetaan hitaaksi**, vaikka uudistamistyötä tehdään jatkuvasti. Myös Brass ym. (2018, s. 4) toteavat, että tällä hetkellä kehitettävät standardit, jotka koskevat IoT:n tietoturvaa, kehittyvät suhteellisen hitaasti. Akkretoitujen auditoijien kokemukset ISO 27001-standardin uudistustyön hitaasta uudistustyöstä tukee aiempaa tutkimusta. He toteavat samalla, että ISO 27001-standardin päivitysprosessi on parhaillaan käynnissä.

Myös Traficom (2019) tukee näkemystä hyväksyttämisprosessin hitaudesta. Traficom (2019) toteaa omilla internet-sivuillaan, että standardoinnin on vaikea vastata alan nopeasti muuttuviin teknisiin tarpeisiin tehokkaasti. Asian nostaa esiin myös Brass ym. (2018, s. 4)

omassa tutkimuksessaan. Heidän näkemyksensä tukee edellä mainittujen näkemyksiä ja toteavat standardin olevan merkityksellinen internetin tietoturvalle. Turvallisuuden hallintastandardi ei kuitenkaan koske Brass ym. (2018, s. 4) mielestä kaikkia IoT-ekosysteemin komponentteja. Muodollisten standardien kehityksen he näkevät IoT-tietoturvassa hitaaksi (Brass ym., 2018, s. 4).

Akkretoitujen auditoijien näkemyksen mukaan käytettävän **auditointikriteeristön kohdentaminen** auditoitavaan kohteeseen, aiheuttaa myös paljon huolta ja pohdintaa auditoijien keskuudessa. Tämän johdosta haastatteluissa nousi esiin, soveltuuko käytettävä standardi auditoitavaan kohteeseen ja onko tarvetta käyttää lisästandardin vaatimuksia, jotta auditoinnista saadaan hyväksyttävä lopputulos. Tällaisen tilanteen voi aiheuttaa haastattelujen perusteella auditoitavan kohteen tiedon määrä, laatu sekä tiedon arvo, minkälaista dataa järjestelmä sisältää. Myös Traficomin (2019) näkemyksen mukaan standardi antaa tarvittavan viitekehyksen ja riskiperustaisen näkymän organisaation tietoturvallisuuden hallintaan. ISO 27001-standardi tukee myös kansallisia vaatimuksia (Traficom, 2019). Samanlaisen näkemyksen tuovat esiin omassa tutkimuksessaan Saleem ym. (2018), auditoijien on määritettävä organisaation turvallisuusmenettelyt ja todisteet hyvien turvallisuuskäytäntöjen noudattamisesta.

Pakottava tietoturva-asetuksen tarpeellisuus herätti keskustelua akkretoitujen auditoijien ja yritysasiantuntijoiden keskuudessa. Auditoijat nostivat esiin ISO 27001- standardin vaatimukset, jossa tulee huomioida lakimääräiset vaatimukset. Auditoijat pitivät hyvänä vapaaehtoista tietoturvallisuuden hallintajärjestelmän standardia, koska se soveltuu lähes kaikille yrityksille koosta ja toimialasta riippumatta. Pakottavan tietoturva-asetuksen nähtiin nostavan organisaatioiden tietoturvatasoa. Sitä vastoin yritysasiantuntijoiden keskuudessa pakottava tietoturva-asetus aiheutti eriäviä näkemyksiä. EU:n kyberturvallisuusasetuksen ei nähty tuovan suuria vaikutuksia yrityksen toimintaan lähitulevaisuudessa. Traficomin (2019) näkemyksen mukaan EU:n kyberturvallisuusasetuksen sertifioinnissa tullaan käyttämään jo olemassa olevia standardeja niin teknisissä vaatimuksissa kuin arviointimenettelyissäkin.

Akkretoidut auditoijat sekä yritysasiantuntijat toivat esiin yhteisen näkemyksen kansainvälisen ja kansallisen auditointikriteeristön ongelmista. Heidän näkemyksensä mukaan kansalliset kriteerit eivät ole linjassa kansainvälisten kriteeristöjen kanssa, jolloin

tilanne johtaa organisaatioiden kohonneisiin audiointikustannuksiin. Tällaisessa tapauksissa on myös mahdollista, että auditoitavalta organisaatiolta kysytään samoja asioita usean eri auditoijien toimesta, hieman eri näkökulmasta.

5.2 Tietoturvan ja riskienhallinnan moninaisuus

Tutkimuksessa tunnistettiin erilaisia tietoturvan riskienarviointiin ja muutoksenhallintaan liittyviä heikkouksia. Akkretoitujen auditoijien haastatteluissa esiin nousi vahvasti esiin **heikot arviointimenetelmät riskienhallinnassa** ja **muutoksenhallinnassa.** Näihin auditoijien näkemyksen mukaan ei kiinnitetä tarpeeksi huomioita. Riskienhallinta voi olla pinnallista, ja sen merkitystä ei tarpeeksi ymmärretä organisaatiossa. Tämä voi johtua organisaation osaamisen vajeesta ja resurssipulasta. Toiseksi heikkojen arviointimenetelmien puutteeseen johtaa myös kokonaisuuksien ja suojattavan omaisuuden ymmärtäminen organisaatiossa. Muutoksien mahdollinen vaikutus hallintajärjestelmässä saattaa jäädä usein huomioimatta muutoksen vähäpätöisyyden vuoksi ja muutosta ei nosteta riskienhallintamenettelyyn, koska organisaatio ei ymmärrä muutoksen vaikutusta. Tämän saman asian esiin nostaa Nurse ym. (2017, s. 5), he mainitsevan IoT:n riskienarvioinnin olevan riittämätöntä ja lisäksi tilannetta pahentaa riskienarvioinnin osittain ajoittainen luonne.

Riskienarviointia heikentää myös **ennakoinnin puute** muutoksenhallinnassa. Organisaatiot eivät auditoijien mukaan osaa ennakoida tarpeeksi hyvin tulevia muutoksia ja reagoida niihin. Näitä muutoksia aiheuttaa uudenlainen teknologia ja menetelmät, joihin vaikuttaa organisaation henkilökunnan **osaamisen puute**. Kuten Nurse ym. (2017, s. 8) toteavat, muutosvauhdin olevan niin nopea, että riskienarviointimenettelyn toimenpiteet eivät ole ajan tasalla. Samanlaisen näkemyksen toivat esiin myös yritysasiantuntijat. Myös **elinkaarenhallinta** nousi esiin haastatteluissa, johon ei asiantuntijoiden mukaan osata kiinnittää tarpeeksi huomiota. Auditoijat nostivat esiin myös palveluna ostaminen, jolloin palvelun tarjoaja tarjoaa tuotteelleen elinkaarihallinnan maksua vastaan ja vastaa laitteeseen kohdistuvasta tietoturvasta sekä ylläpidosta.

Seuraavaksi käsittelen IoT:n heterogeenisiin alustoihin liittyviä ongelmia, joita nousi esiin haastatteluista. **Osaamisen puute** nousi yhdeksi isoksi asiaksi myös IoT- alustoissa niin auditoijien kuin myös yritysasiantuntijoiden näkemyksissä. Ensinnäkin ympäristön tuntemus

ei ole toivotulla tasolla ja tämä vaikuttaa IoT- järjestelmän kokonaisuuksien ymmärtämiseen. **Kokonaisuuksien ymmärtämistä** vaikeuttaa huomattavasti IoT:n heterogeeninen toimintaympäristö ja siihen liittyvät moninaiset ominaisuudet sekä toimintaympäristö, tämä vaikuttaa myös hankittaessa IoT-ympäristöä. Myös Nicolescu ym. (2018, s. 346) näkevät omassa tutkimuksessaan IoT:n tarkoittavan eri asioita eri toimijoille, jolloin kokonaisuuden ymmärtäminen on tärkeää.

Yritysasiantuntijat nostivat **turvallisuuden** tärkeään osaan IoT-järjestelmissä, kun taas auditoijat näkevät turvallisuuden tulevan riskienhallinnan ja muutoksenhallinnan kautta IoT-hallintajärjestelmään. Ensinnäkin IoT-järjestelmäalustan hankkijalla pitäisi olla erittäin hyvä osaaminen ja näkemys hankittavan järjestelmän ominaisuuksista, millaiset rajapinnat hankittava järjestelmä muodostaa, sekä mitä mahdollisia riskejä niiden kautta voi muodostua. Toisena, miten järjestelmän tietoturva on hoidettu ja millaisilla ominaisuuksilla. Samaan tulokseen ovat tulleet myös Atlam ja Wills (2019, s. 124) ja toteavat, että tällä hetkellä tehokkaan ja luotettavan tietoturvan rakentaminen on yksi tärkeimmistä asioista.

Akkretoidut auditoijat mainitsevat ISO 27001- standardin soveltuvan kaikille yritykselle, mutta tuovat myös esiin huolen **A-liitteen soveltuvuudesta** käytännössä, jota pidetään yleisesti puutteellisena. Yritysasiantuntijat näkivät asian myös riittämättömänä samalla tavalla kuin auditoijat. Auditoijilla ja yritysasiantuntijoilla oli yhteneväinen näkemys lisästandardin käytöstä, jolla voidaan varmistaa riittävä IoT-alustan tietoturva ja hallinnointi menetelmät. Auditoijat muistuttivat, että A-liitteen päivitys on parhaillaan käynnissä.

5.3 Auditoinnin vaikutus hallintajärjestelmään

Tutkimuksessa tunnistettiin erilaisia haasteita, joita nousee esiin auditoinnin yhteydessä yritysten IoT- järjestelmien tietoturvanhallinnassa. Ensimmäiseksi haasteeksi nousi akkretoitujen auditoijien mukaan erilaiset IoT-ympäristön muodostamat **rajapinnat** ja niihin pysähtyvä hallintajärjestelmän vastuu. Tämä nähdään ongelmallisena, koska osa hallinnoitavasta järjestelmästä jää auditoinnin ulkopuolelle tai auditointi katkeaa rajapintaan, koska toista järjestelmää hallinnoi ulkopuolinen organisaatio.

Yritysasiantuntijoiden näkemyksen mukaan auditoijalle jää suuri vastuu löytää IoT-laitteita sisältävän hallintajärjestelmän rajapinnat sekä löytää raja, joka kuuluu hallintajärjestelmään. Tällöin puhutaan **auditoinnin laajuudesta**, joka muodostaa oman haastekokonaisuuden. Tätä näkemystä tukee myös Brassin ym. (2018, s. 4) johtopäätös, jossa he toteavat IoT-ekosysteemin topologian ja sen suuren sovellusalueen haastavan nykyisen muodollisen standardin toiminnan. Ongelmaksi nousee heidän mukaansa datan liikennöintirajojen yhteydet ja palvelujen rajattavuus. Auditoijat nostavat myös esiin uudenlaisen rajapintoihin liittyvän elementin auditoitavien asiakkaiden tietoturvavastuista ja esittävät kysymyksen, mistä kaikesta asiakas ottaa tietoturva vastuun. Samaan viittaavat Oracevic ym. (2017) omassa tutkimuksessaan, jossa he mainitsevat heterogeenisilla IoT- komponenteilla olevan samat tietoturvallisuusvaatimukset kuin kaikilla muillakin hallintajärjestelmään liittyvillä laitteilla, jotka ovat tietoverkkojen kautta yhteyksissä toisiinsa.

Haastateltavat nostivat esiin myös jatkuvuuden hallintaan liittyvät ongelmat, joihin ei auditoijien näkemyksen mukaan kiinnitetä tarpeeksi huomiota. **Jatkuvuudenhallinnan** tärkeyden ymmärtäminen nousee esiin pilvipalvelujen yhteydessä. Suuret palveluntarjoajat mainostavat haastateltavien mukaan palvelun olevan aina käytettävissä. Tähän liittyy kuitenkin maantieteellisiä haasteita, jotka muodostuvat eri maiden ylittävistä tietoliikenneverkoista ja vaikuttavat jatkuvuudenhallintaan. Tätä tukee myös Radanliev ym. (2019) näkemys siitä, että IoT-järjestelmät ulottuvat useille alustoille ja ylittävät maantieteellisiä rajoja, joille tarvitaan jatkuvuussuunnitelmat.

Auditoijat nostavat esiin jatkuvuudenhallintaan liittyvän **osaamisen**. Organisaatioista puuttuu kyvykkyys ajatella tarpeeksi laaja-alaisesti mahdollisesti muodostuvaa ongelmaa. Jatkuvuudenhallintaan liittyy myös tunnistettujen riskien loppuun vieminen ja riskien tason saattaminen hyväksyttävälle tasolle tai kokonaan poistaminen. Radanliev ym. (2019b, s. 3) toteavat, että jaetun riskin ymmärtäminen on elintärkeää riskienarvioinnissa, koska riskin arvioitu kohde voi vaihdella merkittävästi.

Johtamisen kysymykset nousivat haastatteluissa keskeiseen asemaan IoT-hallintajärjestelmien ylläpidossa. Akkretoidut auditoijat nostavat esiin puutteellisen johtamisen ja ylimmän johdon ymmärtämättömyyden standardin vaatimuksista. Puutteellisella vastuunkannolla nähtiin olevan suora vaikutus hallintajärjestelmän **teknisen**

osaamisen tasoon sekä **resursointiin**, näillä on vaikutusta yrityksen tekniseen ja organisatoriseen osaamiseen. Tämä korostuu haastateltavien näkemyksen mukaan myös puutteellisena hankintaosaamisena, jolloin ei välttämättä osata huomioida tarvittavia asioita hankintaa tehdessä.

Myös **koulutuksen puutteet** nousevat esiin organisaatiossa, jotka hallinnoivat IoT:tä sisältäviä hallintajärjestelmiä. Yrityksen onkin tärkeää Oracevicin ym. (2017) mukaan ymmärtää turvallisuutta määrittelevät ominaisuudet. Myös mainetekijät vaikuttavat auditoijien näkemyksen mukaan positiivisesti hallintajärjestelmän tietoturvatasoon. Auditoijat näkevät auditoinnin johtavan positiiviseen vaikutukseen yritysten tietoturvaponnisteluissa ja niiden ei nähdä haluavan negatiivista mainetta mahdollisten tietoturvahyökkäysten aiheuttamista ongelmista.

5.4 Johtopäätökset

Tämän tutkimuksen tavoitteena oli selvittää miten ISO 27001- standardin vaatimukset ottavat huomioon ja vastaavat IoT- alustojen ympäristön riskeihin. Avainhenkilöitä tässä tutkimuksessa ovat akkretoidut auditoijat, jotka työssään auditoivat yritysten tietoturvallisuuden hallintajärjestelmiä. Myös yritysasiantuntijoiden näkemysten avulla selvitettiin ISO 27001- standardin soveltuvuutta IoT- laitteita sisältävien tietoturvallisuuden hallintajärjestelmiin. Tutkimuksen teoreettinen viitekehys muodostui alan viimeisimmistä kansainvälisistä tutkimuksista. Tutkimustyön empiirinen osuus muodostui akkretoitujen auditoijien ja yritysasiantuntijoiden haastatteluista.

Tässä alaluvussa vastataan kahteen alatutkimuskysymykseen, jonka jälkeen siirrytään käsittelemään päätutkimuskysymyksen johtopäätöksiä.

Ensimmäinen alatutkimuskysymys:

Miten IoT-alustojen heterogeenisyys otetaan huomioon auditoinneissa?

Tutkimuksen johtopäätöksinä todetaan IoT-alustojen heterogeenisyyden olevan auditoinneissa kaiken kaikkiaan vaikeasti tunnistettavissa oleva asia. Heterogeenisyys aiheuttaa riskien hallintaongelmia auditoinnin kohteena oleville organisaatioille.

Auditoinneissa yritetään yleisesti tunnistaa heterogeenisen Iot-laiteympäristön riskikohtia, jotka voisivat vaikuttaa tietoturvahyökkäyksen toteutumiseen. Lisäksi auditoinneissa selvitetään, minkälaisia tietoturvan hallinnointikeinoja ja turvallisuuskontrolleja hallintajärjestelmään sisältyy. Valmistajien kyvykkyys tuottaa turvallisuuskontrolleja valmistamiinsa laitteisiin koetaan ongelmana organisaatioissa.

Tämän tutkimuksen tekijä näkee kuitenkin IoT-alustojen heterogeenisyyden olevan paljon suurempi ja monimutkainen ongelma. Tutkijan mukaan IoT-alusta voi koostua hyvin erilaisista laitteista, joiden tarkkaa toimintaa, ominaisuuksia ja liitettävyyttä ei järjestelmää käyttävä organisaatio tunne tai tunnista. Nämä seikat eivät tule järjestelmällisesti esille auditoinneissa. Auditoinneissa hallintajärjestelmien rajaus myös aiheuttaa heterogeenisissä IoT-alustoissa turvallisuuspuutteita. Auditoijat eivät pääse analysoimaan kaikkia niitä toiminnallisuuksia, jotka liittyvät datan liikkeisiin muihin järjestelmiin hallintajärjestelmistä. Tämä tarkoittaa, että osa kyseiseen IoT-ekosysteemiin liittyvistä laitteista jää auditoinnin ulkopuolelle ja voi aiheuttaa vakavan tietoturvaongelman. Tämä ongelma tulee myös esille, jos kumppaniorganisaatio hallinnoi osaa IoT-järjestelmästä ja auditointia ei uloteta koko IoT-ekosysteemin alueelle.

IoT-alustojen heterogeenisyys olisi paremmin hallittavissa, jos kaikki laitteet ja järjestelmät olisivat hallintajärjestelmän piirissä. Tämä edesauttaisi kokonaisuuden parempaa hahmottamista. Toisaalta kaikkien laitteiden ja järjestelmien liittäminen hallintajärjestelmän piiriin muuttuu vaikeasti hallittavaksi kokonaisuudeksi. Lisäksi auditoitavan kokonaisuuden kasvaessa, myös kustannukset nousevat. Kokonaisten IoT-ekosysteemien auditointi nähdään tärkeänä. Auditoijalla onkin suuri vastuu huomioida hallintajärjestelmän auditoinnissa kaikkien kriittisten laitteiden ja järjestelmien sisällyttäminen auditointiin, ilman että osia kokonaisuudesta rajataan ulkopuolelle.

Kokonaisuuksien huomioimisessa on tärkeää kiinnittää erityistä huomiota rajapintoihin ja pieniltäkin vaikuttavien komponenttien huomioimiseen järjestelmänhallinnassa. IoT-ekosysteemin hahmottaminen kokonaisuutena nouseekin erittäin tärkeään rooliin. Tämä vaatii asiantuntijoilta jatkuvaa osaamisen kehittämistä ja kykyä ympäristön muutoksien havainnointiin myös ennakoiden. Kokonaisuuksien ymmärtäminen ja riittävä osaamisen taso auttavat tunnistamaan IoT-alustojen heterogeenisyyden erityispiirteitä.

Toinen alatutkimuskysymys

Minkälaisia riskien havainnointimenetelmiä IoT-pilvipalveluissa on mahdollista käyttää?

Tutkimuksen johtopäätöksinä todetaan, että riskien havainnointimenetelmiä tulee ajatella uudella tavalla IoT-pilvipalveluympäristössä. IoT-alustojen riskienhallintaan voidaan vaikuttaa tehokkaalla muutoksenhallinnalla ja havainnointikyvyllä. Uudenlaisessa ajattelutavassa pienimmätkin muutokset yrityksen toiminnassa tai toimintaympäristössä pitää analysoida riskipohjaisesti. Tähän ajattelutapaan liittyy myös jatkuva muutoksenhallinnan ennakoiva ajattelumalli, proaktiivisuus. Proaktiivisessa mallissa muutoksia hallinnoidaan ja analysoidaan ennakoivasti, toisaalta myös ennakkoluulottomasti.

Organisaation riskienhallintaa tukee parhaalla tavalla ketterä muutoksenhallinta. Ketterässä muutoksenhallinnassa tehdään jatkuvaa valvontaa, tunnistamista sekä havaintoja toimintaympäristön muutoksista. Kun taas jaksollisuus korostuu vanhan mallisessa riskienhallinnassa. Tässä yhteydessä on hyvä nostaa esiin organisaation henkilökunnan mahdollisuus tehdä havaintoja. Organisaation henkilökunta voidaan myös velvoittaa havainnoimaan poikkeavuuksia tietty määrä henkilöä kohden vuodessa, kuitenkin niin, että samasta juurisyystä ei saisi muodostua uutta havaintoa. Henkilökunnan on ymmärrettävä mitä teknologiaa, tietoa tai laitteita suojattavaan kokonaisuuteen sisältyy, jotta yksilö kykenee sisäistämään hallittavan kokonaisuuden. Organisaation on panostettava omassa toiminnassaan henkilökunnan riittävään osaamiseen. Henkilökunta on keskeisessä roolissa riskien jatkuvassa havainnoinnissa.

Muutoksenhallintaa pitääkin ajatella moniulotteisesti ja avarakatseisesti. Muutoksen tunnistaminen voi johtaa uuden hyökkäysmenetelmän tai haavoittuvuuden tunnistamiseen hallittavassa ympäristössä. Muutoksenhallinnassa on mahdollisuus käyttää apuna myös tekoälyä, jolloin osan järjestelmän analytiikasta toteuttaa kone. Tällaisesta toiminnasta saadaan riskienhallintaan monipuolisia hyötyjä sekä nopeutetaan vasteajan muutoksien havainnointia. Lisäksi pienetkin muutokset IoT-ekosysteemissä on mahdollista havaita ja ekosysteemiin kohdistuviin hyökkäysyrityksiin on mahdollisuus reagoida nopeasti. Tekoälyn avulla tapahtuva valvontaa voidaan toteuttaa kellon ympäri.

Päätutkimuskysymys:

Miten ISO 27001- standardin vaatimukset vastaavat IoT-alustojen riskeihin?

Tutkimuksen johtopäätöksenä ISO 27001-standardin vaatimuksista vastaamaan IoT-alustojen riskeihin voidaan todeta seuraavaa:

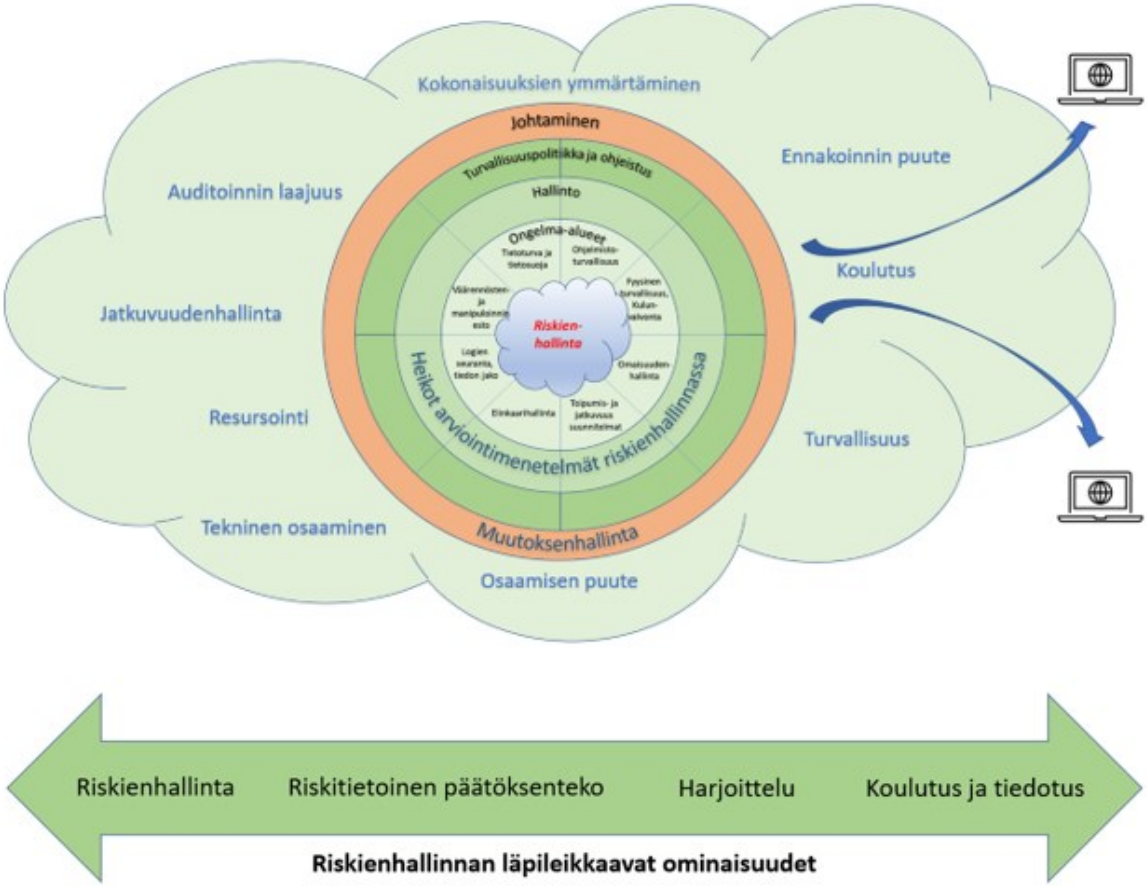
ISO 27001-standardin tietoturvallisuuden hallintajärjestelmä on kestänyt hyvin ajan tasalla, koska standardia on päivitetty säännöllisin väliajoin. ISO 27001-standardin joustavuuden johdosta, standardi soveltuu monelle toimialalle sekä erikokoisille yrityksille tietoturvallisuuden hallintajärjestelmäksi. Kuitenkin ISO 27001-standardin kansainvälinen uudistamisprosessi koetaan hitaaksi, kun sitä verrataan IoT-ekosysteemien erittäin nopeaan kehittymisvauhtiin. Tämä aiheuttaa haasteita standardin vaatimuksiin ja niiden soveltamiseen asiakasympäristössä.

Edellä oleva analyysi ohjaa seuraaviin päätelmiin. IoT-laitteita sisältävä ympäristö muodostaa hyvin erilaisia tietoturvaan liittyviä ongelmia, joihin standardi ei suoraan ota kantaa. ISO 27001-standardin liitettä A, pidetään yleisesti riittämättömänä IoT- palveluympäristöjen riskien tarkasteluun. Tässä nähdään tarve mahdolliselle lisästandardin käytölle. Ongelmana on, että IoT-laitteita sisältäville järjestelmille ei ole tällä hetkellä olemassa standardia, joka huomioisi riittävän monipuolisesti heterogeenisen IoT-ekosysteemin tuomat erityispiirteet ja haasteet tietoturvallisuuden hallintajärjestelmissä. Tämä johtaa tilanteeseen, jossa joudutaan turvautumaan joissain tapauksissa sopivaan apustandardiin organisaatiossa sekä auditoinnissa.

ISO 27001-standardia käyttävän yrityksen pitää kiinnittää huomiota standardin riskienhallinnan kontrollien ennakkoluulottomaan ja laaja-alaiseen soveltamiseen omassa toimintaympäristössään (kuva 2). Yrityksen johdolla tulee olla myös ymmärrys oman toimintaympäristön kattavasta muutoksenhallinnasta, standardin käytettävyydestä ja vaatimusten soveltuvuudesta omassa toimintaympäristössään. Turvallisuuspolitiikan ja ohjeistuksen tulee olla organisaation johdon hyväksymä ja johto on myös sitoutunut niiden soveltamiseen ja käyttöön. Riskienhallinnan arviointimenetelmien osalta, yrityksen tulee kiinnittää erityistä huomiota niiden monipuolisuuteen ja ennakoitavuuteen. Tällä hetkellä

riskienarviointimenetelmiä voidaan yleisesti kutsua heikoiksi, niiden kapea-alaisuuden vuoksi. Yrityksen johdon tulee tarjota riittävät resurssit ja varmistaa IoT-ekosysteemin hallinnollinen sekä tekninen osaaminen. IoT-ympäristö muuttuu nopeasti ja vaatii asiantuntijoilta jatkuvaa koulutusta ja ymmärrystä jatkuvuudenhallinnan tarpeista.

Kuva 2. IoT-ekosysteemien auditoinneissa huomioitavat keskeiset asiat, soveltaen. (DiMase ym., 2015, s. 294)



Johdon näkökulmasta kokonaisuuksien ymmärtäminen on keskeisessä asemassa. Auditoinnin laajuus tulee ulottaa mahdollisuuksien mukaan koko IoT-järjestelmään liitettyjen komponenttien laajuudelle, myös liityntäpinnat kumppaneiden järjestelmiin tulee huomioida. IoT-järjestelmään kohdistuva turvallisuustason nostaminen mahdollistuu oikeilla hallinnointimenetelmillä. Kun johto panostaa ISO-sertifikaattiin, se panostaa samalla jatkuvuuden hallintaan ja tulevaisuuden liiketoimintaan.

5.5 Tulosten yleistettävyys ja käytännön suositukset

Tämän tutkimuksen tulokset ovat kohtalaisen hyvin yleistettävissä erilaisten organisaatioiden IoT-alustojen riskien tunnistamiseen, jotka nousevat esiin ja joita vaaditaan ISO 27001-standardin tietoturvallisuuden hallintajärjestelmässä. Tulosten yleistettävyyttä tukee myös IoT-laitteiden jatkuva kasvu erilaisissa tietoturvallisuuden hallintajärjestelmissä, joissa tietoturvaan liittyvät näkökohdat tulee huomioida. Akkretoitujen auditoijien ja yritysasiantuntijoiden haastatteluissa esiin tulleet näkemykset vahvistavat yleistä käsitystä IoT-alustojen tietoturvariskien hallinnan heikosta tasosta organisaatioissa. Tätä näkemystä vahvistavat myös kansainvälisten tutkimusten antamat saman suuntaiset tulokset.

Tulosten yleistettävyys antaa mahdollisuuden käyttää tätä tutkimusta apuna suunniteltaessa organisaatioiden IoT-hankkeita. Tutkimus antaa viitteitä mihin organisaation kannattaa kiinnittää huomiota IoT-alustoja rakentaessaan. Se antaa myös uusia ajatuksia ja tukea organisaatioiden sisäisten ja ulkoisten IoT-riskien tunnistamiseen.

Tutkimusten tulosten perusteella voidaan suosittaa organisaatioille ISO 27001-standardin tietoturvallisuuden hallintajärjestelmän IoT-riskienhallinnassa seuraavia asioita, joihin tulee kiinnittää erityistä huomiota:

- Kokonaisuuksien ymmärtäminen: IoT-ekosysteemin rajapintojen tunnistaminen oman organisaation toiminnan kannalta, huomioiden myös yhteistyökumppaneiden rajapinnat.
- Muutoksenhallinta: organisaatioiden tulee kiinnittää huomiota oman muutoksenhallinnan toimivuuteen, sen syvyyteen sekä riskienhallinnan kykyyn huomioida organisaatiossa tapahtuvien muutosten vaikutusta toimintaympäristöön.
- Osaaminen: osaamisen ja osaamisympäristöjen hyödyntäminen omassa liiketoiminnassa niin, että saatua tietoa voidaan hyödyntää omassa toimintaympäristössä. Osaamisella tarkoitetaan hallinnollista ja teknistä järjestelmäosaamista.
- Ennakointi: Riskienhallinnassa ja muutoksenhallinnassa heikkojen signaalien havaitseminen ja tunnistaminen omassa toimintaympäristössä on tärkeää. Esiin

nousevia asioita analysoidaan ja arvioidaan niiden vaikutusta organisaation omaan toimintaan.

Mahdollisena jatkotutkimuksena nostetaan esiin johtamisen näkökulma, erityisesti johdon sitoutuminen ISO 27001-standardin vaatimuksien ymmärtämiseen vaatii lisätutkimusta. Johto on mukana auditointitilanteissa, koska vastuu tietoturvasta kuuluu ylimmälle johdolle. Tietoturvallisuuteen ja riskienhallintaan liittyvät kysymykset jäävät kuitenkin johdon näkökulmasta usein etäisiksi ja irrallisiksi, koska asian tärkeyttä ei välttämättä ymmärretä. Tietoturvan hallinnointi on voitu myös vastuuttaa alemmalle organisaatiotasolle. Tämä voi johtua johdon omasta kiinnostuksen ja osaamisen puutteesta tai vaihtoehtoisesti johto ei esimerkiksi saa asiantuntijoilta tarvitsemaan tietoa johtamisen tueksi, jolloin kokonaisuudenhallinta jää puutteelliseksi.

Johtamiseen liittyvänä jatkotutkimuksena nostetaan esiin myös IoT-ekosysteemin auditointien rajapintojen hallinnointi. Johdolla pitäisi olla vahva näkemys pilvialustojen rajapintoihin liittyvistä toiminnoista. Nämä rajapinnat muodostavat epästandardin heterogeenisen toimintakentän, jossa muodostuu helposti toimivuusongelmia sekä tietoturvariskien huomattavaa kasvua. Organisaation pitää tuntea toimintaympäristönsä kokonaisuutena ja huomioida erilaiset rajapinnat.

Tämän tutkimuksen tekijä kokee oman IoT-ekosysteemeihin liittyvän tietoturvaosaamisensa kasvaneen tutkimuksen edetessä. Uusimmat tieteelliset artikkelit ovat lisänneet tutkijan ymmärrystä IoT-ekosysteemien moninaisuudesta. Auditoijien ja yritysasiantuntijoiden haastattelut nostivat esiin heterogeenisen IoT-ympäristön riskienhallintaan liittyvät ongelmat. Teorian ja käytännön rinnakkain asettaminen auttoivat tutkijaa ymmärtämään IoT-riskienhallinnan analysointia paremmin jokapäiväisessä työskentelyssä. Kokonaisuuksien hahmottaminen IoT-ekosysteemissä on lisääntynyt ja tätä tietoa on mahdollista hyödyntää omassa työympäristössä.

LÄHTEET

Atlam, H,. Wills, G. (2019). IoT Security, Privacy, Safety and Ethics, 123–149.

Banafa, A. (2018). Eight Trends of the Internet of Things in 2018. *IEEE, Internet of Things newsletter*, Tammikuu 9, 2018. https://iot.ieee.org/newsletter/january-2018/eight-trends-of-the-internet-of-things-in-2018

Botta, A., De Donato, W. Persico, V. & Pescapé, A. (2015). Integration of Cloud computing and Internet of Things. Future Generation Computer Systems 56, 684–700. https://iotiran.com/media/k2/attachments/Integration_of_Cloud_computing_and_Internet_of_Things_A_survey.pdf

Brass, I., Tanczer, L., Carr, M., Elsden, M. & Blackstock, J. (2018). Standardising a Moving Target: The Development and Evolution of IoT Security Standards. 1–9. https://discovery.ucl.ac.uk/id/eprint/10045804/1/PETRAS_Submission_Ref-0083_FullPaper.pdf

DiMase, D., Collier Z. A., Heffner, K. & Linkov. I. (2015) Systems engineering framework for cyber physical security and resilience. *Environ Syst.Decis* 35, 291–300. Systems_engineering_framework_for_cyber_20151115-3624-xb424a.pdf (d1wqtxts1xzle7.cloudfront.net)

Duncan, B. & Whittington, M. (2016). Enhancing Cloud Security and Privacy: The power and the Weakness of the Audit Trail. *Cloud Computing 2016: The Seventh International Conference on Cloud Computing. GRIDs and Virtualization*, 125–130. cloud_computing_2016_6_20_20063.pdf (abdn.ac.uk)

Eskola, J. & Suoranta, J. (2014). *Johdatus laadulliseen tutkimukseen.* Kustannusosakeyhtiö Vastapaino, Tampere

Gisladottir, V., Ganin, A.A., Keisler, J. M., Kepner, J. & Linkov, I. (2017). Resilience of Cyber Systems with Over- and Underregulation. *Risk Analysis, Vol. 37, No. 9,* 1644–1651 Resilience of Cyber Systems with Over- and Underregulation - Gisladottir - 2017 - Risk Analysis - Wiley Online Library

Hejazi, H., Rajab, H., Cinkler, T., Lengyel, L. (2018). Survey of Platforms for Massive IoT. http://real.mtak.hu/85019/1/Future_IoT_2018_paper_16.pdf

Hirsjärvi, S. & Hurme, H. (2009). *Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö*. Yliopistopaino. Helsinki.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2016). *Tutki ja kirjoita*. Kustannusosakeyhtiö Tammi, Helsinki.

Ikonen, H-M. (2017). Puhelinhaastattelu. Teoksessa M. Hyvärinen, P. Nikander & J. Ruusuvuori (toim.) *Tutkimushaastattelun käsikirja* (270–284). Kustannusosakeyhtiö Vastapaino.

Jha, A., Sunic, M. (2014). Security considerations for Internet of Things, L&T Technology Services. https://www.ltts.com/sites/default/files/whitepapers/2017-07/whitepaper_security-considerations-for-internet-of-things.pdf

Kananen, J. (2008). Kvali. *Kvalitatiivisen tutkimuksen teoria ja käytänteet*. Jyväskylän ammattikorkeakoulun julkaisuja 93. Jyväskylän yliopistopaino.

Kananen, J. (2010). *Opinnäytetyön kirjoittamisen käytännön opas,* Jyväskylän ammattikorkeakoulu, Jyväskylä

Koskinen, I., Alasuutari, P. & Peltonen, T. (2005). *Laadulliset menetelmät kauppatieteissä.* Kustannusosakeyhtiö Vastapaino, Tampere

König, S., Schiebeck, S., Schauer, S., Latzenhofer, M., Mayer, P. & Fitzpatrick G. (2017). Deliverable 3. Internet of Things Risk Analysis and Assessment. Project Risiot: Market analysis and risk assessment to accelerate the adoption of the internet of things in Austrian enterprises. https://images.idc-cema.com/mail-image/1091307/risiot_internet_of_things_risk_analysis_and_assessment.pdf

Kyberturvallisuusasetus, Euroopan parlamentin ja neuvoston asetus EU:n kyberturvallisuusvirastosta ENISA:sta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista 2017/0225.

MacGillivray, C. (2016). The Platform of Platforms in the Internet of Things, White paper, IDC Analyse the future , 1–7. https://iotslam.com/wp-content/uploads/2016/06/IDC-Study-IoT-Platform-of-Platforms.pdf

Matheu-Garcia, S. N., Hernández-Ramos, J. L., Skarmeta, A. & Baldini, G. (2018). Risk-based Automated Assessment and Testing for the Cybersecurity Certification and Labelling of IoT Devices. 1–38. https://www.researchgate.net/profile/Sara_Nieves_Matheu_Garcia/publication/327099163_Risk-based_Automated_Assessment_and_Testing_for_the_Cybersecurity_Certification_and_Labelling_of_IoT_Devices/links/5be4197a92851c6b27af571a/Risk-based-Automated-Assessment-and-Testing-for-the-Cybersecurity-Certification-and-Labelling-of-IoT-Devices.pdf

Metsämuuronen J. (2009). *Tutkimuksen tekemisen perusteet ihmistieteissä*. International Methelp oy, Helsinki.

Mills J. & Birks M. (2014). *Qualitative methodology*. First published. British Library Cataloguing in Publication data. Great Britain: Ashford.

Mineranda, J., Mazhelisb, O., Xiang Suc, X. & Tarkomaa, S. (2016). A gap analysis of Internet-of-Things platforms, *Preprint submitted to Computer Communications, Special issue on the Internet of Things: Research challenges and Solutions*, 1–15. 1502.01181.pdf (arxiv.org)

Nicolescu, R., Huth, M., Radanliev, P., De Roure, D. (2018). Mapping the values of IoT, *Journal of Information Technology*, 33, 345–360. Mapping the values of IoT (springer.com)

Nurse, J. R. C., Creese, S. & De Roure, D. (2017). Security risk assessment in Internet of Things Systems. IT Professional (IT Pro) September/October 2017 Special Issue on “Establishing Trust in the Internet of Things”. 1–9. https://arxiv.org/ftp/arxiv/papers/1811/1811.03290.pdf

Nurse, J. R. C., Radanliev, P. Creese, S. & De Roure, K. C. (2018). If you can´t understand it, you cant´t properly assess it! The reality of assessing security risk in Internet of Things system. 1–9. https://arxiv.org/pdf/1806.10906.pdf

Oracevic, O., Dilek. S., Ozdemir, S. (2017). Security in Internet of Things: A Survey. ResearchGate, https://www.doc.ic.ac.uk/~livshits/classes/CO445H/reading/Security-in-Internet-of-Things-A-Survey.pdf

Pasquier, T., Singh, J., Powles, J., Eyers, D., Seltzer, M., Bacon, J. (2017). Data provenance to audit compliance with privacy policy in the Internet of Things. *Pers Ubiquit Comput*, 22:333–344. ubi-2017.pdf (harvard.edu)

PwC Suomi (2016). Luottamus ja esineiden internet.

Radanliev, P., De Roure, C., Cannady, S., Montalvo, R.M., Nicolescu, R. & Huth, M. (2018). Economic Impact of IoT Cyber Risk- Analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. https://arxiv.org/ftp/arxiv/papers/1810/1810.10322.pdf

Radanliev, P., De Roure, D., Nurse, J. R. C., Nicolescu, R., Huth, M., Cannady, S. & Montalvo, R. M. (2018a). Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-Things in Industry 4.0. Living in the Internet of Things: Cybersecurity of the IoT, 28-29 March 2018, 1–6. https://kar.kent.ac.uk/67464/1/Integration+of+Cyber+Security+Frameworks+Models+and+Approaches+for+Building+Design+Principles+for+the+Internet_of_Things+in+.pdf

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S. & Burnap, P. (2018b). Future developments in cyber assessment for the internet of things. *Computer in Industry 102,* 14–22.

Radanliev, P., De Roure, D. C., Maple, C., Nurse, J. R.C., Nicolescu, R. & Ani, U. (2019). Cyber Risk in IoT Systems.

Radanliev, P., De Roure, D., Nurse, J. R. C., Nicolescu, R., Huth, M., Cannady, S. & Montalvo, R. M. (2019a). Cyber risk impact assessment. Assessing the risk from the IOT to the digital economy. Oxford e-Research Centre. 1–11.

Radanliev, P., De Roure, D., Nurse, J.R.C, Nicolescu, R., Huth, M., Cannady, S., Mantilla Montalvo, R. (2019b). Cyber Security Framework for the Internet-of-Things in Intrustry 4.0. 1–7.

Radanliev, P., De Roure, D. C., Nurse, J. R.C., Montalvo R. M., Cannady, S., Santos, O., Maddox, L. Burnap, P. & Maple, C. (2020). Future developments in standardisation of cyber risk in the Internet of Things (IoT). SN Applied Sciences (2020) 2:169. *Springer Nature journal*.

Ranta, J. & Kuula-Luumi, A. (2017). Haastattelun keruu ja käsittelyn ABC. Teoksessa M. Hyvärinen, P. Nikander & J. Ruusuvuori (toim.) *Tutkimushaastattelun käsikirja*. Kustannusosakeyhtiö Vastapaino.

Riahi, A., Natalizio, E., Challal, Y., Mitton, N. & Iera, A. (2014). A systemic and cognitive approach for IoT security. HAL, 1–6. A systemic and cognitive approach for IoT security (inria.fr)

Ruusuvuori, J. & Nikander P. (2017). Haastatteluaineiston litterointi. Teoksessa M. Hyvärinen, P. Nikander & J. Ruusuvuori (toim.) *Tutkimushaastattelun käsikirja*. Kustannusosakeyhtiö Vastapaino.

Saleem, J., Hammoudeh, M., Raza, U. & Adebisi, B., Ruth, A. (2018). IoT standardisation - Challenges, perspectives and solution. https://www.researchgate.net/profile/Jibran_Saleem/publication/327332700_IoT_standardisation_challenges_perspectives_and_solution/links/5b8c6eb3299bf1d5a73a02f9/IoT-standardisation-challenges-perspectives-and-solution.pdf

SFS-EN ISO 27001:2017 (2017). Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmä. Vaatimukset, 1–54, Suomen standardisoimisliitto SFS ry.

Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini,A. (2014). Security, privacy and trust in Internet of Things: The road ahead, *Computer Networks 76,* 146–164. https://www.idi.ntnu.no/emner/tdt49/p10-secpriv.pdf

Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., Coen-Porisini, A. (2016). A secure and quality-aware prototypical architecture for the Internet of Things, *Information systems* 58, 43–55.

Sicari, S., Rizzardi, A., Miorandi, D. & Coen-Prisini, A. (2018). A Risk Assessment Methodology for the Internet of Things, 1–17.

Singh, J., Pasquier, T., Bacon, J., Ko, H. & Eyers, D. (2016). Twenty Security Considerations for Cloud-Supported Internet of Things. *Internet of Things Journal*, IEEE 3 (3), 1–16. https://dash.harvard.edu/bitstream/handle/1/35349952/iot-2016.pdf?sequence=1

Toivanen, L. (2017). IoT-integraatioalustat, Centria-ammattikorkeakoulu, raportteja ja selvityksiä, 21, 1–42. https://www.theseus.fi/bitstream/handle/10024/123510/978-952-7173-21-3+%28PDF%29.pdf?sequence=3

Traficom (2019). Luottamuksen lähteillä. Näkökulmia tietoturvan standardointiin ja sertifiointiin. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

Ziegler, S., Skarmeta, A., Bernal, J., Kim, E.E., Bianchi, S. (2017). ANASTACIA: Advanted Networked Agents for Security and Trust Assessment in CPS IoT Architectures, ANASTACIA_Advanced_Networked_Agents_for_Security_and_Trust_Assessment_in_CPS_IoT_Architectures.pdf (anastacia-h2020.eu)

Liite 1: Gioia-metodi

Miten hallintajärjestelmän auditoinneissa huomioidaan IoT:tä sisältävät asiat?			
Raakamateriaali	1. tason konsepti	2. tason konsepti	yhdistetyt dimensiot
A1 Mielenkiintoinen tämä rajapintaan pysähtyvä vastuu, varsinkin kun ne laitteet pelkästään pökkäs palveluun dataa analysoitavaksi ja sieltä ei niin kuin pilvestä mitään käskytetty	Rajapintaan pysähtyvä vastuu	IoT-rajapintaan pysähtyvä vastuu. Suojattavan omaisuuden sijainti ja vastuiden ja valtuuksien määrittäminen	**Rajapinnat**
A2 mahdollistaako tämmöinen IoT-järjestelmä pääsyä kenties vielä arvokkaampaan dataan	Pääsy arvokkaaseen dataan		
A4 assetti luettelo, mitä asetteja on, missä ja minkä tyyppisiä, miten niihin liittyvät vastuut ja valtuudet hoidettu, niiden käyttö ja sijainti	Suojattavan omaisuuden sijainti, tyyppi, vastuut ja valtuudet		
A1 Talotekniikan laitteistoa siellä (pilvipalvelu) sitten säädetään, jossa oli tämä IoT-puoli, mutta IoT-puoli ei ollut auditoinnin skoupissa millään tavalla	IoT-ekosysteemin laajuus	IoT-ekosysteemin laajuus auditoinnissa. Tiedon ja omaisuuden huomiointi auditoinnin laajuuden avulla	**Auditoinnin laajuus**
A2 Jos ne ovat kattavuusalueella on IoT-järjestelmä niin silloin pitää ottaa huomioon, mutta tosiaan miten ne huomioidaan	IoT-ekosysteemin laajuuden huomioiminen		
A3 Riskienhallinnassahan on se eheys, saatavuus ja luottamuksellisuus sekä se tiedon ja omaisuuden hallinta, miten ne on hoidettu	Tiedon ja omaisuuden hallinta laaja-alaisesti		

Liite 2: Haastattelukysymykset

Haastattelukysymykset

Lainsäädäntö

1. Miten EU:n kyberturvallisuusasetus tulee vaikuttamaan toimintaanne?
2. Onko pakottavalle tietoturva-asetukselle tarvetta?
3. Tunnistatko ristiriitaa kansallisien ja kansainvälisien tietoturva-auditointien käytössä? (vahti, Katakri, Pitukri)

IoT-alustat

4. Ovatko turvallisuusnäkökohdat mielestäsi selkeitä arvioitaessa IoT:tä sisältäviä alustoja?
5. Monissa kansainvälisissä tutkimuksissa viitataan IoT-alustoja sisältävien laitteiden tietoturvastandardien puutteeseen. Miten näet tämän auditoijan näkökulmasta?
6. Kuinka ajantasainen ISO 27001 -standardi on mielestäsi IoT-alustojen tietoturva-auditoinnissa?
7. Onko ISO 27001 standardi mielestäsi riittävä monipuolinen IoT-alustojen auditointityökaluksi?

Riskienhallinta ja tietoturva

8. Miten mielestäsi pystytään huomioimaan kaikki uudenlaiset tietoturvariskit, joita IoT-heterogeeninen järjestelmäympäristö aiheuttaa?
9. Miten riskienarviointi mielestäsi otetaan huomioon jatkuvasti muuttuvassa IoT-järjestelmissä?
10. Pitäisikö IoT-alustoilla mielestäsi ottaa käyttöön uudenlaisia riskien havainnointimenetelmiä?
11. Onko muutostenhallinta mielestäsi huomioitu tarpeeksi IoT-järjestelmien riskienhallinnassa?

Auditointi

12. Miten hallintajärjestelmän auditoinnissa huomioidaan mielestäsi IoT:tä sisältävät asiat?
13. Mitä tietoturva-aukkoja tunnistetaan mielestäsi IoT-pohjaisen pilvipalvelun auditoinneissa (ISO 27001)?
14. Miten ISO 27001-auditoinnissa mielestäsi vaikuttaa asiakasyrityksen osaamisen puute?